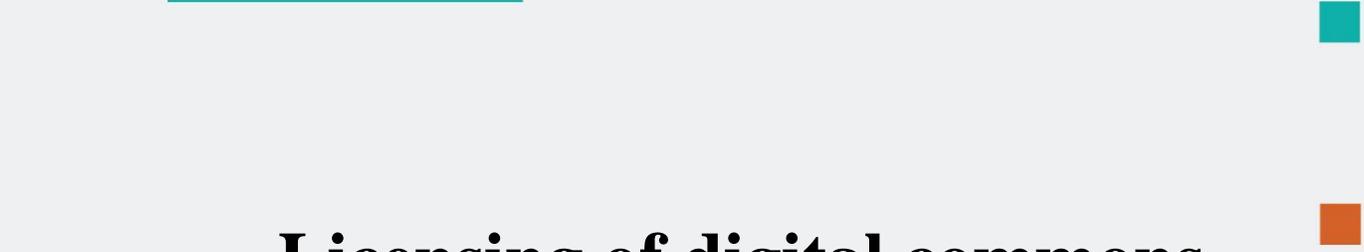
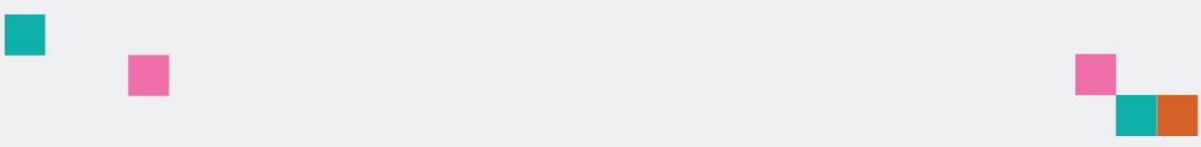




# decode



## Licensing of digital commons including personal data



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

D1.9 Licensing of digital commons including personal data

Version Number: V1.0

Lead beneficiary: POLITO

Due Date: September 30th, 2018

Author(s): Eleonora Bassi, Marco Ciurcina, Juan Carlos De Martin, Selina Fenoglietto (POLITO)

Editors and reviewers: Antonio Calleja (UOC), Stefano Lucarelli (CNRS), Francesca Bria (IMI)

Dissemination level:		
<b>PU</b>	Public	<b>X</b>
<b>PP</b>	Restricted to other programme participants (including the Commission Services)	
<b>RE</b>	Restricted to a group specified by the consortium (including the Commission Services)	
<b>CO</b>	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: 30/09/2018**

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

# Executive summary

This document provides a review of the licensing options for digital data commons, even for the case that data commons include personal data.

The review starts with the analysis of the most common licensing procedures, free licenses and best tools that allow the releasing of artifacts avoiding licenses' incompatibility and possible violations of third party's rights. Then it recalls the necessity to distinguish the different kinds of data managed and processed through DECODE services, in order to identify the proper license for each of them.

The analysis continues focusing on digital commons made of personal data and on how they can be licensed.

At the end, the document offers an initial set of smart rules to be adopted by the pilots or other services based on DECODE OS in order to strengthen users control on data commons, a table for evaluating the compatibility of free licenses to be adopted for DECODE artifacts, and a Data Commons Privacy Pledge, that is a pool of voluntary standard commitments for strengthening data privacy rights and digital commons values.

This deliverable shall be read in combination with: D1.8 "Legal framework for digital commons DECODE OS and legal guidelines" which provides legal references and concepts, such as copyright, IPRs rights, licenses, personal data, and so on, that are analyzed in this deliverable; D2.1 "Multidisciplinary Framework on Commons Collaborative Economy" for the definition of digital commons; D1.4 "First Version of the DECODE Architecture"; D4.9 "Design & implementation interface for smart rules"; D3.5 "Initial definition of Smart Rules and Taxonomy". In addition, to read this text could be useful to check the legal domain taxonomy provided within D1.8.

# Contents

Motivation and structure of the document .....	5
Acronyms Table .....	6
1. Introduction: Digital Commons Licensing for DECODE .....	7
2. DECODE products and outputs: licensing procedures and tools .....	8
2.1 Procedures, tools and information .....	8
2.2 How to check artifacts to be reused .....	10
2.3 How to check releasing artifacts .....	12
3. DECODE datasets: how to license datasets as digital commons .....	13
3.1 Different kind of datasets .....	13
3.2 Licensing steps .....	14
3.2.1 How to check datasets to be reused .....	15
3.2.2 How to check releasing datasets .....	15
3.2.3 Smart rules for IPRs management of releasing datasets .....	15
4. Digital Commons and Personal Data .....	16
5. References .....	19
Annex A: Initial Set of Smart Rules (SR) for DECODE datasets .....	20
Annex B: Compatibility test for free licenses .....	39
Annex C: Digital Data Commons Privacy Pledge .....	45
Digital Data Commons Privacy Pledge .....	45

# Motivation and structure of the document

This deliverable reviews options for the licensing of data as digital commons, including personal data. It also provides an initial set of smart rules to be adopted by the pilots in order to fulfill law requirements and to strengthen users control on data commons.

This document consists of 5 sections, 3 annexes. and an acronyms table.

**Section 1** "Introduction: Digital Commons Licensing for DECODE" introduces to the necessity of identifying specific legal tools for the licensing of DECODE project's artifacts as digital commons

**Section 2** "DECODE products and outputs: licensing procedures and tools" is a review of the common licensing procedures, free licenses and best tools that allow the releasing of artifacts avoiding licenses' incompatibility and possible violations of third party's rights.

**Section 3** "DECODE datasets: how to license datasets as digital commons" firstly examines the different kinds of data managed and processed through DECODE services, secondly identifies the different steps to be followed to license those datasets as digital commons.

**Section 4** "Digital Commons and Personal Data" analyses how to make digital commons with personal data, recommending the undertaking of a Digital Data Commons Privacy Pledge, that provides a pool of voluntary standard commitments for strengthening data privacy rights and digital commons values.

**Annex A** "Initial set of Smart Rules (SR) for DECODE datasets" provides 3 boxes.

**Box 1** includes examples of SR for datasets of data not including personal data (e.g.: application of a license).

**Box 2** includes examples of SR for datasets with personal data (e.g.: SR for the provision of information and consent and withdrawal of consent).

**Box 3** is a table that identifies the objects of SR for datasets including personal data, and distinguishes the different actions, roles and time of the operation (table: Declarative entitlements).

**Annex B** is a **Compatibility test for free licenses**.

**Annex C** is the **Digital Data Commons Privacy Pledge**.

References are available in **Section 5**.

# Acronyms Table

Acronym	Meaning
BSD	Berkeley Software Distribution
CC	Creative Commons
DECODE OS	Decode Operating System
DLT	Distributed Ledgers Technology
EPL	Eclipse 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
MIT	Massachusetts Institute of Technology
SR	Smart Rule
UDP	User Data Provider (user that adopts a SR to provide his personal data)
UDR	User Data Recipient (user that adopts a SR to get access to personal data to use it (becoming data controller)

# 1. Introduction: Digital Commons Licensing for DECODE

The analysis of the legal frameworks that concerns the creation of digital commons has to be expanded to the review of legal tools necessary for sharing them and exploiting their potentiality. This document examines free licenses, SR and other legal declarations and commitments concurring to define the boundaries of digital commons' data regime.

DECODE will create digital data commons from data produced by individuals and devices. People will be able to decide which personal data they want to share into the commons, and on which basis<sup>1</sup>.

As analyzed in D1.8 "Legal frameworks for digital commons DECODE OS and legal guidelines" and D2.1 "Multidisciplinary Framework on Commons Collaborative Economy" DECODE embraces the idea of digital data commons as a shared resource made accessible and intentionally open, like free software and wikipedia.

To make it possible DECODE will use legal tools and technical solutions operated through SRs to license data as commons, managing user preferences for data sharing and empowering them to control what they share, with whom and under which conditions.

In order to set up the best tools for sharing data as commons, a crucial point is to specify the (legal) features of data to be shared, such as data not including personal data, company data, data covered by IPRs, data and metadata from mobile apps, data and metadata from IoT services, personal data, and so on.

The first step is transparency over what data is held by whom, and the ability to authorize any sharing while understanding the legal implications.

As undertaken in the Consortium Agreement (Section 9.8.3), the DECODE Project is releasing its outputs (such as design architecture of the DECODE DLT, software, organizational processes, data and datasets) as open as possible fostering the creation of digital data commons, and allowing users to choose the licensing regime they prefer in order to share data through DLT based services.

<sup>1</sup> DECODE data commons vision and rationale is outlined by Project Coordinator Francesca Bria in this article: <https://www.theguardian.com/commentisfree/2018/apr/05/data-valuable-citizens-silicon-valley-barcelona>

## 2. DECODE products and outputs: licensing procedures and tools

The products and outputs of DECODE project can be described as “Digital common output”, that Deliverable D2.1 “Multidisciplinary Framework on Commons Collaborative Economy”, defines as: “an immaterial common that can exist in a digital support (e.g. free software, open design, an mp3 file with an open license, etc.)” (Section 2.3.2.2, p. 50).

Deliverable D1.8 “Legal frameworks for digital commons DECODE OS and legal guidelines”, identifies the strategies to be adopted within DECODE project to license the different artifacts produced by the project (see Section 2.3), following the provisions of the Consortium Agreement (Section 9.8.3). D1.8 distinguishes between:

- a) software and other artifacts to be deployed in the DECODE OS and DECODE Nodes (see D1.8, Section 2.3.1 “Free licenses for the DECODE technology”);
- b) datasets resulting from the use of the DECODE technology (see D1.8, Section 2.3.2 “Free licenses for the data shared with DECODE”).

Furthermore, D1.8, Section 3.1 “Recommendations on the design of DECODE OS” provides recommendations on licensing of software and other artifacts of DECODE OS.

When datasets do not include personal data, the use of free licenses is a sufficient measure to foster the creation of digital commons as discussed in Section 3.2.

The issue becomes more complex when the datasets include personal data; this case will be analyzed in Section 4.

For the creation and distribution of DECODE artifacts we suggest to follow the good practices of the sector.

### 2.1 Procedures, tools and information

Regarding software artifacts, good practices and tools are well documented and widespread, so that free software developing teams usually organize their work following such practices and using such tools: there is no need to change already established good practices and tools as long as they allow achieving the expected results.

It is worth mentioning the “Open Compliance Program” of the Linux Foundation<sup>2</sup> that provides a list of publications and tools the support in organizing a compliance procedure.

The Linux Foundations supports the SPDX standard<sup>3</sup> that provides a common format for information about free software licenses and copyrights (SPDX Tools that provide translation, comparison, and verification functionality are also available). The Linux Foundations supports also the OpenChain Project<sup>4</sup>, a project that, among others, provides the OpenChain Specification, a set of requirements for compliance programs.

FOSSology<sup>5</sup> is a free software license compliance software system and toolkit that allows running license and copyright scans.

Many other tools are available (some commercial, some free software)<sup>6</sup>.

Information about free software licenses is easily accessible from different sources and good points to start with are:

- the GNU project website that lists licenses that comply with the free software definition, provides FAQ about the GNU licenses and other useful information<sup>7</sup>;
- the Open Source Initiative website that lists licenses that comply with the Open Source Definition and provides other information<sup>8</sup>;
- the Wikipedia website that provides information about most of the free software licenses (e.g., [https://en.wikipedia.org/wiki/Apache\\_License](https://en.wikipedia.org/wiki/Apache_License)) including comparison of free and open-source software licenses<sup>9</sup>;
- the Choose a License website<sup>10</sup> and the tldrLegal website<sup>11</sup> that provide information about some of the most well-known free licenses and the obligations to be complied with according to each of them.

Regarding creative works not consisting in software (like datasets, texts, images and pictures), it is worth mentioning the Creative Commons website that, among others, makes available a tool that helps in choosing a CC license<sup>12</sup>.

2 See <https://compliance.linuxfoundation.org/>.

3 See <https://www.spdx.org/>.

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

5 See <https://www.fossology.org/>.

6 Among the tools available as free software we can mention Ninka, a license identification tool (see <http://ninka.turingmachine.org/>) and the Open Source License Checker (see <https://sourceforge.net/projects/oslc/>).

7 See <https://www.gnu.org/licenses/>.

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

9 See [https://en.wikipedia.org/wiki/Comparison\\_of\\_free\\_and\\_open-source\\_software\\_licenses](https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses).

10 See <https://choosealicense.com/>.

11 See <https://tldrlegal.com/>.

12 See <https://creativecommons.org/choose/>.

Vice versa, practices and tools for artifacts not consisting in software are not so well established and widespread.

Notwithstanding such complexity, some general provisions can be suggested.

For all artifacts, including datasets, we suggest to adopt a procedure to deal with the following issues:

- a) Checking artifacts to be reused and their license, then
- b) Choosing the proper license for releasing artifacts and verifying their compliance with licenses of reused artifacts.

## 2.2 How to check artifacts to be reused

Free licenses (of software, of other artifacts and of datasets) set up obligations on who distributes (on physical media or online) copies or modifications (so-called *patches*) of free artifacts or who distributes products that include components with free licenses that have to comply with these obligations<sup>13</sup>.

In some cases, even the offer of software as a service (so-called SaaS) may imply the need to comply with some of the obligations imposed by free software licenses (for instance, if you use network copyleft software on the server<sup>14</sup> or if the user must use on his device free software distributed by the service provider).

Who intends to carry out a complex project, reusing several artifacts licensed with different free licenses, should analyze how the different components interact to avoid the risk of incompatibility.

Various copyleft licenses impose a set of obligations which are typical of this type of licenses on who distributes the artifact. Nonetheless, those obligations are not always the same: they vary depending on the specific license adopted.

For example, among the free software licenses some of them require:

- to make the software available also in source format (e.g., GNU-GPL and MPL),
- to include information on the installation of the software (e.g., GNU-GPL and EPL),
- for the case you change the software, to make available also the original version (e.g., MPL and GNU-GPL),
- to not impose further obligations on the user limiting the further distribution of the software (eg, GPL and MPL).
- to hold harmless the software contributors from any damages resulting from the distribution of products that include the software itself (eg, the EPL).

<sup>13</sup> See above Section 2.1 and, particularly, notes 9 and 10.

<sup>14</sup> See Deliverable D1.8 “Legal frameworks for digital commons DECODE OS and legal guidelines”, Section 1.2.2.2 (“Free licenses characteristics”), p. 30.

There are also other obligations concerning all types of free licenses, even those non-copyleft, which also vary from license to license.

First of all, practically all free licenses require redistribution of the artifact with a copyright notice.

Secondly, some licenses require to distribute the artifact with other information to be drafted according to specific indications (which vary from license to license).

For example, some licenses require:

- to include the license text (eg, MIT and Apache licenses),
- to give credit to the authors of the artifact (eg, original MITv1 and BSD licenses),
- for the case you change the artifact, to indicate which changes have been introduced (e.g., GNU-GPL and Apache license).

Moreover, some free software licenses provide for obligations with respect to patent rights for invention that may be held by the user of free software. For instance, some free software licenses contain an explicit license of the patent rights of the software vendor (e.g., GNU-GPLv3) or contributor (e.g., GNU-GPLv3, MPLv2 or Apache license). It is also believed that some free software licenses (e.g., GNU-GPLv2 and modified BSD) contain an implicit patent license that applies to software distributors and contributors.

Some licenses contain also so-called "retaliation" clauses which, under certain conditions, determine the termination of the free software license if the licensee claims the infringement of a patent (e.g., MPL, GNU-GPLv3 and Apache license) that interferes with the use of the software.

Finally, it is important to remember that the violation of the free software licenses can terminate the license, with the consequent need to "do something" to reacquire the right to use the software according to the terms of the same free software license (e.g., GNU-GPL - in different ways for GNU-GPLv2 and GNU-GPLv3 - MPL and EPL).

To avoid the violation of the obligations set up by free licenses it is useful to adopt some simple precautions.

In particular:

- adopting contracts with suppliers of artifacts to make them responsible for compliance with the obligations set up by the free licenses,
- encouraging internal developers to adopt version control systems,
- adopting procedures and tools that make easier choosing the free license to adopt for each artifact to be distributed,
- identifying the subjects that are responsible for the compliance with the obligations set up by the free licenses,
- foreseeing that, prior to the distribution, artifacts (acquired from third parties or developed internally) are controlled by identified managers.

As mentioned above, adopting the OpenChain Specification could be helpful to achieve these goals. Sometimes it could be also useful to use artifacts analysis tools (like FOSSology) to automatically acquire information on licenses and copyright notices of the artifacts that are reused and distributed.

## 2.3 How to check releasing artifacts

To distribute an artifact, a license has to be chosen.

It's therefore important to verify that the license to be adopted for the releasing artifact complies with the licenses of the artifacts eventually reused.

Some copyleft licenses<sup>15</sup> are incompatible with each other. Then, in order to carry out a complex project, reusing artifacts licensed with different free licenses, it is crucial to analyze how the different components interact to avoid the risk of incompatibility.

In order to make easier this analysis, a compatibility test, with a list of steps to be performed, is provided in Annex B "Compatibility test for free licenses".

This test can apply to software and other artifacts, including datasets (some special remarks for datasets will be made in Section 3.2.2).

Even if the compatibility test is not passed, it's still possible to ask to (and obtain from) the author(s) of the artifact to be reused that is available under the terms of an incompatible license to license the same artifact under the terms of a different free license and/or to add an exception to such license. The viability of this option depends on different circumstances (how many reused artifacts adopt incompatible licenses, if the author(s) of such artifacts own the rights necessary to license the artifacts under different licenses or to provide for an exception, etc.) but, ultimately, it depends on the fact that the author(s) reply positively to the request.

15 See Deliverable D1.8 ("Legal frameworks for digital commons DECODE OS and legal guidelines"), Section 1.2.2.2 ("Free licenses characteristics"), p. 30.

# 3. DECODE datasets: how to license datasets as digital commons

## 3.1 Different kind of datasets

Different kind of datasets are processed throughout the DECODE Project.

Firstly, DECODE processes

1) data necessary to the running of the DLT services; this is the case of technical data that is independent from data related to each specific service (or pilot) based on DECODE and data provided by users. Differently from the former, those latter are discretionary with respect to the functioning of the DLT DECODE OS.

Secondly, each DECODE pilot (or service that will be based on DECODE OS technology) manages datasets from different sources:

2) datasets shared autonomously by users<sup>16</sup>;

3) datasets collected and released by public sector administrations or companies (we are referring more precisely to public sector bodies<sup>17</sup>), that are freely and openly available to the public;

4) datasets (belonging to users and/or public sector administrations) gathered automatically by IoT devices connected with DECODE OS.

Thirdly, each DECODE pilot (or service) will produce new datasets:

5) datasets generated by analytics based on other datasets (e.g. datasets sub 2), sub 3), sub 4)), or datasets derived from a combination or a selection of datasets sub 2), sub 3), sub 4).

In order to figure out the correct legal regime for those different kinds of data (with particular attention to copyright and other IP rights), it is useful to distinguish among:

(a) datasets stored on the ledger, and

16 Within DECODE, users are potentially all residents (in Amsterdam and Barcelona) who are eligible to take part in testing the technology developed in the project (see <https://decodeproject.eu/>).

17 According to the definition set up by the European Directive on public sector information Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, Article 2(1), ""public sector body" means the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law". It is important to recall that all these bodies (but see the exception posed within the PSI Directive from 2003 and the new PSI Directive from 2013) are required to release their data as open data.

(b) datasets shared by users (specially, pilot participants), or available through DECODE services, which are linked to the ledger but that are not stored on it.

Finally, another distinction concerning privacy regimes shall be made between

(i) datasets that include personal data<sup>18</sup>, and

(ii) datasets made of data not including personal data.

All those distinctions affect and set up the legal framework to be compliant with and the rights to make safe where they are released and licensed.

## 3.2 Licensing steps

As discussed in D1.8 “Legal framework for digital commons DECODE OS and legal guidelines”, in some cases, datasets are subject to copyright, related rights and other rights<sup>19</sup>.

The rights clearance procedure described in Section 2 could be adopted for licensing datasets, even though some remarks are to be made.

The tools mentioned in Section 2 were usually designed for software and there are not *ad hoc* tools for datasets.

The information available about how to apply free licenses to datasets (how to deal with compatibility issues, etc.) is not as widespread as the information that refers to software. Nevertheless the checks to be made are the same. Then, the procedure described in Section 2 has to be followed also for datasets in order to:

a) check datasets (and their content) to be reused and their license, then

b) choose the proper license for releasing datasets and verify their compliance with licenses of reused datasets (and their content).

Moreover, we should take into account the proper characteristics of datasets and free licenses applied to datasets.

18 Here we recall the definition of personal data set up by Article 4(1) of the GDPR: “‘personal\_data’ means any information relating to an identified or identifiable natural person (‘data subject’); 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”. For a more detailed analysis of the implication of such definition within DECODE and, more generally, DLTs, see D1.8 “Legal framework for digital commons DECODE OS and legal guidelines”, Section 1.3, p. 35.

19 See D1.8 “Legal framework for digital commons DECODE OS and legal guidelines”, Section 2.3.2, p. 60.

The particular case where datasets include personal data is analyzed in Section 4, where is described the possibility to adopt SRs to comply with the obligations provided by the GDPR.

### 3.2.1 How to check datasets to be reused

The considerations made in Section 2.1 apply to datasets with the following specific remarks.

In a nutshell, datasets are complex objects. This implies that different IPRs can apply to the dataset as a whole and to specific parts of the datasets (for instance, to specific data that is part of a dataset) in different ways.

The first step is, therefore, to check exactly what is the copyright regime of the dataset and of its components, and if there are other IPRs insisting on it (e.g. *sui generis* right on datasets), third parties rights, or other legal constraints (e.g. statistical secrecy)<sup>20</sup>.

### 3.2.2 How to check releasing datasets

The considerations made in Section 2.2 apply to datasets, with the following specific remarks.

Information on the compatibility of different free licenses when applied to datasets has to be examined from a different perspective, taking into account the specificities of datasets and the particularities about how the right to make modifications and to make compilations is regulated by the different free licenses<sup>21</sup>.

### 3.2.3 Smart rules for IPRs management of releasing datasets

Using a SR to distribute a dataset according to the term of a free license is not necessary *per se*: different methods are available and are used since long time, such as accompanying the artifact with the license's text.

However, the use of a SR for releasing data under the terms of a free license is a technique that offers the possible advantage of automatically strengthening the license within a DLT environment.

In annex A is provided an example of SR to distribute data according to a free license (box 1).

20 For a more detailed analysis of the different rights and ownerships that could be affect data and datasets, see D1.8 "Legal framework for digital commons DECODE OS", Section 1, p. 7.

21 A good tool is the compatibility table provided by MORANDO F., *Legal interoperability: making Open Government Data compatible with businesses and communities*, J LIS.it. Vol.4, n.1 (January 2013), DOI: 10.4403/jlis.it-5461 (see <https://www.jlis.it/article/view/5461>).

## 4. Digital Commons and Personal Data

In some cases a person may want to share digital data commons built on personal data (e.g., the anonymous vote results of DECODE DDDC pilot) and even share her personal data as digital data common (e.g., contributing to Wikipedia with nickname or IP address). DECODE offers instruments, architectural, software and legal, for making it feasible and compliant with laws.

Despite the fact, as it was recommended in D1.8, that the first good practice, when dealing with personal data and DLTs, is not to store personal data on the DLT (at least in permissionless DLT, until technology development, interpretation of the GDPR and standard legal solutions are not definitely able to allow legal compliance and rights safeguard), DECODE offers, nonetheless, the possibility to share personal data as digital data commons exploiting the architecture of DLTs, cryptography, privacy design strategies, without any storage of personal data on the distributed ledger itself.

It is certainly possible to build digital commons made of personal data adopting free licenses (see Section 3 of the present document): a good example of this is Wikipedia, that is formed by contributions made by many persons (tracked by their name, email and/or IP address) and thus formed with voluntarily contributed personal data.

Taking advantage of the DLT, particularly SR, there are new ways to foster data sharing: SRs allow making declarations and commitments, to conclude agreements, and to perform specific actions in order to comply with defined obligations<sup>22</sup>.

Such declarations, commitments, and undertakings do not need to be included within the licenses text: on the one hand, some free licenses do not accept any additional or different terms or condition<sup>23</sup>, on the other hand, free licenses normally do not deal with, and therefore are not overlap with, privacy rights. In short, it is neither useful nor efficient to design new licenses to foster the building of digital data commons including personal data.

It is instead a convenient way to be law-abiding the adoption of SRs (providing information, receiving consent, making easier for the data subject to exercise her rights, etc.), and the adoption of declarations and commitments that could strengthen the power of the data subjects on their personal data.

For these reasons, on one hand, we propose in Annex A an initial set of SRs to be used for managing GDPR compliance (box 2) and, on the other hand, we propose a Digital

<sup>22</sup> The question of different kinds of legal acts (contracts, unilateral acts, etc.) and of their different effects can be deepened starting from Ricolfi M., The new paradigm of creativity and innovation and its corollaries for the law of obligations. In: Peter Drahos-Gustavo Ghidini and Hanss Ullrich, *Kritika: Essays on Intellectual Property*. Vol. I, Edward Elgar, Celftenham, 2015, pp. 134-205.

<sup>23</sup> This is the case, for instance, of CC by SA 4.0, section 7.

Data Commons Privacy Pledge (see Annex C). The Pledge provides a set of commitments that the UDR can undertake.

The UDP could allow UDRs to use her personal data if they make the Pledge.

The Pledge is a privacy enhancing tool that aims both to strengthen the safeguard of data protection and privacy rights in a way that aims to be wider and stronger than as provided by the GDPR, and, at the same time, to enforce the autonomy and the power of each UDP as data subject with the goal of fostering acknowledgment, civic engagement and new scenarios of participation and the production of digital commons.

The Digital Data Commons Privacy Pledge includes a set of standard commitments that increase the benefits provided by GDPR for the data subject (the UDPs) overcoming some limits of GDPR in terms of the data subject's power on her personal data.

Undertaking:

- Art. 2 (Promise to respect privacy), the UDR promises to comply with the GDPR even when this would not be applicable;
- Art. 3 (Data deletion), the UDR strengthens Art. 5(1) point. e) of the GDPR (which, under certain circumstances, allows storing personal data for further periods of time);
- Art. 4 (No further purposes), the UDR strengthens Art. 5(1) point e) (which, under certain circumstances, allows processing personal data for further purposes);
- Art. 5 (List of processors), the UDR strengthens Artt. 13 and 14 of the GDPR (which do not require the provision of the details of the processors)
- Art. 6 (No transfer to Unsafe Place), the UDR strengthens Artt. 42-49 of the GDPR (which, under certain circumstances, allow transfer of the data outside of the European Union even if the UDP did not provide her consent.

Some other provisions of the Digital Data Commons Privacy Pledge include promises that aim at strengthening the power of the data subject in different ways:

- according with Art. 6 (No Unsafe Place), the UDR undertakes to not transfer the personal data to places where privacy rights can be hindered by areas of law not covered by the GDPR (state security, prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, etc.);
- Art. 7 (Notice of disclosure), the UDR strengthens Art. 4(9) of the GDPR (which, not including "public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law", allows further disclosures.
- Art. 8 (Jurisdiction) establishes the exclusive jurisdiction of EU courts;
- according with Art. 9 (Right to claim for the Group of Data Subjects) data subjects can protect each other (claiming rights for and on behalf of others);
- undertaking Art. 10 (Research for the Common Good) the UDR promises to make a digital data commons out of the results achieved performing research activity with the personal data of the data subjects;

- with art. 11 (Personal use exception) an exception is provided for personal use of the data.

The Digital Data Commons Privacy Pledge is not a final text: it is a first draft proposal to be discussed by the communities involved, and eventually modified to provide a text useful and adoptable by a number of persons as wide as possible.

A similar approach could also be applied to the different entities involved in a DLT based service. Likewise, different clauses could be included within the contracts between DLT storers and DLT service provider in order to ensure the undertaking of obligations and responsibilities connected to the proper roles and activities of different actors who run the DLTs services, complying with the provisions of Articles 26 and 28 of the GDPR.

All in all, such kind of legal tools are possible strategies by whoever wants to strengthen and enlarge safeguards, liberties and civic rights, even beyond the privacy domain.

## 5. References

Here follows the list of references of this document.

Bassi E., Ciurcina M., De Martin J. C., Fenoglietto S., Rocchi G., Sagarra Pascual O., Bria F., D1.8 “Legal framework for digital commons DECODE OS and legal guidelines”, 2017, available at <https://www.decodeproject.eu/publications/legal-frameworks-digital-commons-decode-os-and-legal-guidelines>;

Bonelli F., van Dijk T., D4.9 “Design & implementation interface for smart rules”, 2018, available at <https://www.decodeproject.eu/publications/design-and-implementation-interface-smart-rules>;

Danezis G., Bano S., Al Bassam M., Sonnino A., D1.4 “First Version of the DECODE Architecture”, 2017, available at <https://www.decodeproject.eu/publications/decode-architecture-first-version>;

Fuster Morell M., Carballa Smichowski B., Smorto G., Espelt R., Imperatore P., Rebordosa M., Rocas M., Rodríguez N., Senabre E., Ciurcina M., D2.1 “Multidisciplinary Framework on Commons Collaborative Economy” for the definition of digital commons, 2017, available at <https://www.decodeproject.eu/publications/multidisciplinary-framework-commons-collaborative-economy>;

MORANDO F., Legal interoperability: making Open Government Data compatible with businesses and communities, J LIS.it. Vol.4, n.1 (January 2013), DOI: 10.4403/jlis.it-5461, available at <https://www.jlis.it/article/view/5461>;

Ricolfi M., The new paradigm of creativity and innovation and its corollaries for the law of obligations. In: Peter Drahos-Gustavo Ghidini and Hanss Ullrich, Kritika: Essays on Intellectual Property. Vol. I, Edward Elgar, Cheltenham, 2015, pp. 134-205, available at [https://iris.unito.it/retrieve/handle/2318/1559624/133267/Kritika\\_06-ch6\\_tracked.pdf](https://iris.unito.it/retrieve/handle/2318/1559624/133267/Kritika_06-ch6_tracked.pdf);

Roio D., Sachy M., D3.5 “Initial definition of Smart Rules and Taxonomy”, 2018, available at <https://www.decodeproject.eu/publications/initial-definition-smart-rules-and-taxonomy>.

# Annex A: Initial Set of Smart Rules (SR) for DECODE datasets

Annex A contains 3 boxes that describe some SR to be implemented.

The specifications of the SRs are drafted following the behavior-driven development (BDD) methodology<sup>24</sup>.

In these boxes the following definitions will apply:

**“Evidence”**: evidence that a Statement (i) is made by an Identified person or entity, (ii) has a content that cannot be repudiated, and (iii) was made at (or prior to) a certain time.

**“Identified”**: a person or entity that is reasonably identified, according to a standard minimum requirement accepted by the other party of the Transaction.

**“Statement”**: a declaration made by an Identified person or entity.

**“Transaction”**: SR that includes at least the provision of a Statement by one Identified person or entity to a third party.

**“Wallet”**: a structured and searchable database in control of a UDP

## **Box 1:**

Describes the SR to be implemented to allow a UDP to provide to a UDR data that the UDR will use under one (or more) free license(s).

In order to achieve this goal 2 use stories are described:

- 1) UDP selects data and one (or more) free license(s) and makes data available.
- 2) UDR makes a Statement undertaking to use the data according to the free license(s).

## **Box 1 – Story 1**

**Story**: UDP makes available data to be used under one (or more) free license(s).

**As a** UDP

**In order to** provide my data

**I want to** have Evidence that UDR made a Statement by which undertakes to use the data under the free license(s) I selected.

<sup>24</sup> See [https://en.m.wikipedia.org/wiki/Behavior-driven\\_development#Behavioral\\_specifications](https://en.m.wikipedia.org/wiki/Behavior-driven_development#Behavioral_specifications).

**Scenario 1:** UDP selects data and license(s)

**Given** that UDP wants to make available a dataset (or a data stream) under one (or more) free license(s)

**And** she wants to select the data (or the data stream)

**And** select one (or more) free license(s).

**When** I start a session

**Then** I can select the dataset (or the data stream)

**And** the free license(s) to be made available to UDP(s)

**Scenario 2:** UDP makes available data

**Given** that UDP has selected data and one (or more) free license(s)

**And** she wants to allow UDR to access such data provided that UDR makes a Statement undertaking to use the data under the free license(s).

**When** the UDP receives the Statement by which UDR undertakes to use the data under the free license(s) and its Evidence

**Then** the data become accessible by the UDR.

### **Box 1 – Story 2**

**Story:** UDR makes a Statement to access data of a UDP

**As a** UDR

**In order to** access the data of a UDP

**I want to** make a Statement undertaking to use the data under the free license(s) selected by the UDP.

**Scenario 1:** UDR makes a Statement undertaking to use the data under the free license(s)

**Given** that one (or more) UDP(s) made (or are going to make) available data under one (or more) free license(s)

**And** I want to access the data

**When** I start a session

**Then** I select the data

**And** I fill-in my details to become Identified

**And** I make the Statement

**And** the Statement and its Evidence are sent to the UDP

**And** the Statement and its Evidence are stored in the Wallet.

**Scenario 2:** UDR accesses data

**Given** that on (or more) UDP made available data under one (or more) free license(s)

**And** I made a Statement for that data

**And** the UDP received the Statement and its Evidence.

**When** I ask to have access to the data

**Then** I have access to the data.

## **Box 2:**

Describes examples of SRs to be implemented to allow the managing of personal data.

In order to achieve this goal 2 use stories are described:

1) UDR accesses personal data providing information, making pledges, and receiving consent.

2) UDP manages information, pledges and consent using the Wallet.

This is just an initial set of SRs.

Further SRs could be developed following the list of actions indicated in Box 3.

## **Box 2 – Story 1**

**Story:** UDR accesses personal data of a UDP

**As a** UDR

**In order to** access personal data complying with the GDPR

**I want to** provide a UDP with a Statement including information according to Art. 13 GDPR (and eventually a pledge) and, when I decide it is necessary, to receive consent from the UDP.

**Scenario 1:** provide information according to Art. 13 GDPR (and eventually a pledge)

**Given** that I want to receive data from one (or more) UDP(s)

**And** I need to provide information according to Art. 13 GDPR (and eventually a pledge).

**When** I select the data I want to access

**Then** I fill-in the information required by Art. 13 GDPR (and eventually a pledge)

**And** make a Statement including the information (and eventually a pledge).

**Scenario 2:** provide information according to Art. 14 GDPR (and eventually a pledge)

**Given** that I want to access data of one (or more) UDP(s) from a third party

**And** I need to provide information according to Art. 14 GDPR (and eventually a pledge).

**When** I select the data I want to access

**Then** I fill-in the information required by Art. 14 GDPR (and eventually a pledge)

**And** make a Statement including the information (and eventually a pledge).

**Scenario 3:** request consent

**Given** that I estimated that one (or more) purpose(s) of the processing listed in the information require(s) consent from UDP(s) as a legal base

**And** I need to receive such consent in order to process the data for such purpose(s).

**When** I fill-in the information

**Then** for each of the processing purposes that I list, I can indicate that I request consent from the UDP(s).

**Scenario 4:** access personal data

**Given** that I want to access personal data

**And** I want to comply with GDPR

**When** I access personal data

**Then** the UDP(s) receives the Statement with the information according to Artt. 13 or 14 GDPR (and eventually a pledge) and its Evidence.

## **Box 2 – Story 2**

**Story:** UDP manages information (and eventually a pledge) and consent

**As a** UDP

**In order to** empower myself in managing my personal data

**I want to** manage information (and eventually a pledge) from UDR(s) and consent I provide them.

**Scenario 1:** receive information according to Artt. 13 or 14 GDPR (and eventually a pledge)

**Given** that a UDR received personal data from me or any third parties

**And** I want to receive and manage such information (and eventually a pledge).

**When** a UDP receives personal data from me or any third parties

**Then** I receive the Statement with the information (and eventually a pledge) and its Evidence

**And** the Statement with the information (and eventually a pledge) and its Evidence are stored in my Wallet.

**Scenario 2:** UDP provides consent

**Given** that a UDR asked me to provide consent for a specific processing

**And** I want to provide consent.

**When** I receive a Statement and its Evidence requiring me to provide consent

**Then** I provide a Statement with the consent

**And** the UDR receives the Statement with my consent and its Evidence

**And** the Statement with the consent and its Evidence are stored in my Wallet.

**Scenario 3:** UDP denies consent

**Given** that a UDR asked me to provide consent for a specific processing

**And** I do not want to provide consent

**When** I receive a Statement and its Evidence requiring me to provide consent

**Then** I deny consent

**And** the UDR receives the Statement with my denial of consent and its Evidence

**And** the Statement with the denial of consent and its Evidence are stored in my Wallet.

**Scenario 4:** UDP withdraws from consent

**Given** that I provided a consent for a specific processing to a UDR

**And** I want to withdraw consent.

**When** I select the consent stored in my Wallet

**Then** I withdraw consent

**And** the UDR receives the Statement with my withdrawal of consent and its Evidence

**And** the Statement with my withdrawal of consent and its Evidence are stored in my Wallet.

**Box 3:**

is a table that identifies objects of SR for datasets including personal data, and distinguishes the different actions, roles and time of the operation (table: Declarative entitlements).

We included this box in order to provide a list of actions and correlative SR contents to be developed for DLT services that aim at be compliant with GDPR rules.

The table distinguishes: different roles within DECODE, actions to be taken, object of the SR, time when the action have to be taken and the SR have to be executed, the legal reference of the required action.

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>User (Data Provider)</b>	Data Subject	participation to the service	at the registration to the service	agrees to the ToS of the Service Controller, eventually with multiple expressions of agreement		
<b>User (Data Provider)</b>	Data Subject	participation to the service	at any time	contributes to datasets according to open licensing terms		See Box 1
<b>User (Data Provider)</b>	Data Subject	Data access	when data is conferred by the UDP, or when data is requested by another user	defines additional voluntary clauses/requirements for data access (through specific SR)		
<b>User (Data Provider)</b>	Data Subject	Consent	when data is conferred	gives her informed consent to the data processing	Art. 6(1), point (a) and Art. 9(2), point (a)	See Box 2
<b>User (Data Provider)</b>	Data Subject	Consent	when data is requested	does not give her informed consent to the data processing	Art. 6(1), point (a) and Art. 9(2), point (a)	See Box 2
<b>User (Data Provider)</b>	Data Subject	Consent	at any time	withdraws her consent to the data processing	Art. 17(1), point (b)	See Box 2
<b>User (Data Provider)</b>	Data Subject	Data subject rights	at any time	has the right to contact the data controller (service controller or the user who have access to data as data recipient) in order to have information on her rights safeguards according to Articles 15-22 of the GDPR	Articles 15-22	
<b>User (Data Provider)</b>	Data Subject	Data subject rights: right to access	at any time	has the right to obtain from the data controller to have access to the data processed and information related to the data processing	Art. 15	
<b>User (Data Provider)</b>	Data Subject	Data subject rights: right to access	at any time, under specific conditions	has the right to obtain from the data controller to have copy of the data processed	Art. 15	
<b>User (Data Provider)</b>	Data Subject	Data subject rights: right to rectification	at any time, under specific conditions	has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her	Art. 16	

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>User (Data Provider)</b>	Data Subject	Data subject rights: right to erasure (right to be forgotten)	at any time, under specific conditions	has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay	Art. 17	
<b>User (Data Provider)</b>	Data Subject	Data subject rights: right to restriction of processing	at any time, under specific conditions	has the right to obtain from the controller restriction of processing	Art. 18	
<b>User (Data Provider)</b>	Data Subject	Data subject rights: data portability	at any time, under the conditions set by art. 20, GDPR	a. has 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 b. has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided	Art. 20	
<b>User (Data Provider)</b>	Data Subject	Data subject rights: right to object	at any time, under the conditions set by art. 21, GDPR	has the right to object, on grounds relating to his or her particular situation to processing of personal data concerning him or her which is based on point (e) or (f) of <a href="#">Article 6(1)</a> , including profiling based on those provisions	Art. 21	
<b>User (Data Provider)</b>	Data Subject	Data subject rights: automated individual decision-making, including profiling	under the conditions set by art. 22, GDPR	has 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	Art. 22	
<b>User (Data Recipient)</b>	Data Controller	Data access	when user data recipient is entitled according with user data provider licensing terms, conditions, and eventually additional clauses	can access to datasets, according to license terms		See Box 1

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>User (Data Recipient)</b>	Data Controller	Data access	when user data recipient is not entitled according with user data provider licensing terms, conditions, and eventually additional clauses	can not access to datasets, according to license terms		See Box 1
<b>User (Data Recipient)</b>	Data Controller	data sharing	where user data recipient has access to datasets according to license terms	can share datasets, according to license terms		See Box 1
<b>User (Data Recipient)</b>	Data Controller	data sharing	when user data recipient is not entitled according with user data provider licensing terms, conditions, and eventually additional clauses	can not share datasets, according to license terms		See Box 1
<b>User (Data Recipient)</b>	Data Controller	data modification	where user data recipient has access to datasets according to license terms	can modify datasets, according to license terms		See Box 1
<b>User (Data Recipient)</b>	Data Controller	data modification	when user data recipient is not entitled according with user data provider licensing terms, conditions, and eventually additional clauses	can not modify datasets, according to license terms		See Box 1
<b>User (Data Recipient)</b>	Data Controller	data dissemination	where user data recipient has access to datasets according to license terms	can disseminate datasets, according to license terms		See Box 1
<b>User (Data Recipient)</b>	Data Controller	data dissemination	when user data recipient is not entitled according with user data provider licensing terms, conditions, and eventually additional clauses	can not disseminate datasets, according to license terms		See Box 1
<b>User (Data Recipient)</b>	Data Controller	information	at any time when personal data is obtained	provides information to the data subject on the data processing	Artt. 13 and 14	See Box 2
<b>User (Data Recipient)</b>	Data Controller	data processing	at any time	adopts all the obligations of the data controller (like the service controller)	Art. 12	

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>User (Data Recipient)</b>	Data Controller	data processing	at any time	adopts actions and take measures to fulfill data controller obligations (see service controller actions)	Art. 12	
<b>User (Data Recipient)</b>	Data Controller	Communications	without undue delay, pursuing art. 34 of the GDPR	provides communication of the data breach to the data subject	Art. 34	
<b>User (Data Recipient)</b>	Data Subject (see column G)	data processing	at any time	adopts the actions allowed for the role of data subject (see column G)		The user data recipient is a data subject on regards to her participation to the service, such as conferring identification data, and so on (see above rows 3-21)
<b>Service Controller</b>	Data Controller	lawful data processing (consent)	when data is conferred	collects consent (or consents where required) by the (users) data subjects	Art. 6	See Box 2
<b>Service Controller</b>	Data Controller	lawful data processing (consent)	at any time	receives the withdrawal of data subjects' consent to the processing	Art. 6	See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>Service Controller</b>	Data Controller	Information on the data processing	<p>a. at the time when personal data is obtained from the data subject (user);</p> <p>b1. where personal data has not been obtained from the data subject: within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;</p> <p>b2. where personal data has not been obtained from the data subject: if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or</p> <p>b3. where personal data has not been obtained from the data subject: if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed</p>	provides the user (data subject) information on the identity and the contact details of the controllers (for the case of joint controllers) and the essence of the arrangement between joint controllers	Art. 13(1,a)	See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>Service Controller</b>	Data Controller	Information on the data processing	<p>a. at the time when personal data is obtained from the data subject (user);</p> <p>b1. where personal data has not been obtained from the data subject: within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;</p> <p>b2. where personal data has not been obtained from the data subject: if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or</p> <p>b3. where personal data has not been obtained from the data subject: if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed</p>	provides the user (data subject) information on the identity and the contact details of the controller between joint controllers	Art. 26(2)	See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
Service Controller	Data Controller	Information on the data processing	<p>a. at the time when personal data is obtained from the data subject (user);</p> <p>b1. where personal data has not been obtained from the data subject: within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;</p> <p>b2. where personal data has not been obtained from the data subject: if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or</p> <p>b3. where personal data has not been obtained from the data subject: if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed</p>	provides the user (data subject) information on the contact details of the data protection officer, where applicable	Art.13 (1,b)	See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
Service Controller	Data Controller	Information on the data processing	<p>a. at the time when personal data is obtained from the data subject (user);</p> <p>b1. where personal data has not been obtained from the data subject: within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;</p> <p>b2. where personal data has not been obtained from the data subject: if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or</p> <p>b3. where personal data have not been obtained from the data subject: if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed</p>	provides the user (data subject) information on the purposes of the processing for which the personal data are intended as well as the legal basis for the processing	Art. 13(1.c)	See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>Service Controller</b>	Data Controller	Information on the data processing	<p>a. at the time when personal data are obtained from the data subject (user);</p> <p>b1. where personal data have not been obtained from the data subject: within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;</p> <p>b2. where personal data have not been obtained from the data subject: if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or</p> <p>b3. where personal data have not been obtained from the data subject: if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed</p>	provides the user (data subject) information on the recipients or categories of recipients of the personal data, if any	Art. 13(1,e)	See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>Service Controller</b>	Data Controller	Information on the data processing	<p>a. at the time when personal data are obtained from the data subject (user);</p> <p>b1. where personal data have not been obtained from the data subject: within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;</p> <p>b2. where personal data have not been obtained from the data subject: if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or</p> <p>b3. where personal data have not been obtained from the data subject: if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed</p>	provides the user (data subject) information on, where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission		See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
<b>Service Controller</b>	Data Controller	Information on the data processing	a. at the time when personal data are obtained from the data subject (user); b1. where personal data have not been obtained from the data subject: within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; b2. where personal data have not been obtained from the data subject: if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or b3. where personal data have not been obtained from the data subject: if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed	provides the user (data subject) information on the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period		See Box 2
<b>Service Controller</b>	Data Controller	Information on the data processing	where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected	provides the user (data subject) prior to that further processing with information on that other purpose and with any relevant further information	Artt. 13 and 14	See Box 2
<b>Service Controller</b>	Data Controller	Information on the data processing	prior to any further processing, where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected	updates the information provided to the data subject on the data processing	Artt. 13(3) and 14(4)	See Box 2

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
Service Controller	Data Controller	Information	without undue delay and in any event within one month of receipt of the request, pursuing art. 12 of the GDPR	provides information on action taken on a request under <a href="#">Articles 15 to 22</a> to the data subject	Art. 12, 15-22	
Service Controller	Data Controller	Information	without undue delay where personal data are transferred to a third country or to an international organization	provides information of the appropriate safeguards pursuant to Art. 46 relating to the transfer	Art. 46	
Service Controller	Data Controller	Data subject rights: right to access	when the data subject makes request to access to data referring to her, under art. 15, GDPR	shall provide the data subject of a copy of the data	Art. 15	
Service Controller	Data Controller	Data subject rights: right to rectification	at any time, without undue delay, under specific conditions set by art. 16 of the GDPR	shall take all the measures in order to rectify inaccurate personal data concerning the data subject	Art 16	
Service Controller	Data Controller	Data subject rights: right to erasure (right to be forgotten)	without undue delay where the data subject makes request of it under Art. 17 of the GDPR	has the obligation to erase personal data	Art. 17	
Service Controller	Data Controller	Data subject rights: right to restriction of processing	at any time, under specific conditions set by art. 18, GDPR	shall take all the measures in order to restrict the data processing	Art. 18	
Service Controller	Data Controller	Notifications	without undue delay and in any event within one month of receipt of the request	a. communicates any rectification or erasure of personal data or restriction of processing carried out in accordance with <a href="#">Article 16</a> , <a href="#">Article 17</a> (1) and <a href="#">Article 18</a> of the GDPR to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort; b. informs inform the data subject about those recipients if the data subject requests it	Art. 19	
Service Controller	Data Controller	Data subject rights: data portability	under the conditions set by art. 20, GDPR	provides the data subject of the data requested, in a structured, commonly used	Art. 20	

SUBJECT	ROLE	OBJECT	TIME	ACTION	GDPR LEGAL BASE	NOTES
				and machine-readable format		
<b>Service Controller</b>	Data Controller	Data subject rights: right to object	when the data subject objects to the data processing, under art. 21, GDPR	shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims	Art. 21	
<b>Service Controller</b>	Data Controller	Data subject rights: automated individual decision-making, including profiling	when the data subject exercises the right not to be subject to the processing, according to the conditions set by art. 22, GDPR	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.	Art. 22	
<b>Service Controller</b>	Data Controller	Communications	without undue delay, pursuing art. 34 of the GDPR	provides communication of the data breach to the data subject	Art. 34	
<b>Service Controller</b>	Data Controller	Communications	at any time	provides any communication on requests under <a href="#">Articles 15</a> to <a href="#">22</a> and <a href="#">34</a> of the GDPR relating to processing to the data subject	Art. 12(1)	

# Annex B: Compatibility test for free licenses

This compatibility test allows to verify the possibility to develop an artifact (hereinafter “**Target**”) reusing free artifacts (hereinafter “**Reused**”) licensed under a license (hereinafter “**R License**”) and to adopt the license of the Target (hereinafter “**T License**”) avoiding license compatibility issues.

The test is divided in 2 phases.

The steps of the test have to be followed for each Reused.

To list Reused and their R Licenses the following table could be used.

Use (and eventually add) one line for each Reused filling in:

- column “Reused” with the name of the Reused and a link to it, and
- column “R License” with the name of the R License and a link to it.

Reused	R License	Relation	R License Copyleft	R License compatible with T License	Linking R License	R License Exception	T License Copyleft	T License compatible with R License	Linking T License	Exception for T License	Exception for other Reused

## Phase A

Phase A verifies **if the R License allows the reuse under the terms of the T License.**

### Step 1

Fill in column “Relation”.

If the Reused is at least in part based on, or “past and copied” as part of, Target (so that it is “included” in Target and the latter can be considered a modified version of the Reused) fill in **value “I”** in column “Relation”.

If the Reused is a software and it is included at compilation time or called at runtime by Target<sup>25</sup> fill in **value “C”** in column “Relation”.

25 Some communication mechanisms used between two separate programs, like pipes, sockets and command-line arguments, are normally considered not triggering the copyleft effect: “when they are used for communication, the modules normally are separate programs.”

If neither value “I” nor value “C” apply, fill in **value “O”** in column “Relation”.

Then **go to Step 2**.

### **Step 2**

If the value of column Relation is **O**, **the compatibility test is passed**.

If the value of column Relation is **I or C**, **go to step 3**.

### **Step 3**

Fill in column “R License Copyleft”.

If the R License is a copyleft license add value “Yes” in column “R License Copyleft”.

If the R License is not a copyleft license add value “No” in column “R License Copyleft”.

Then **go the step 4**.

### **Step 4**

If the R License is not a copyleft license (**value “No” for column “R License Copyleft”**), **go to Phase B** (Phase A is concluded positively).

If the R License is a copyleft license (**value “Yes” for column “R License copyleft”**), **go to Step 5**.

### **Step 5**

Fill in column “R License compatible with T License”.

If the R License allows licensing a modified version of the Reused including it under the terms of the T License add value “Yes” for column “R License Compatible with T License”.

If the R License does not allow licensing a modified version of the Reused including it under the terms of the T License add value “No” for column “R License Compatible with T License”.

Then **go the step 6**.

### **Step 6**

If the R License allows licensing a modified version of the Reused including it under the terms of the T License (**value “Yes” for column “R License Compatible with T License”**), **go to Phase B** (Phase A is concluded positively).

---

*But if the semantics of the communication are intimate enough, exchanging complex internal data structures, that too could be a basis to consider the two parts as combined into a larger program” (see <https://www.gnu.org/licenses/gpl-faq.en.html#MereAggregation>; for further details see [https://en.wikipedia.org/wiki/License\\_compatibility](https://en.wikipedia.org/wiki/License_compatibility)).*

If the R License does not allow licensing a modified version of the Reused including it under the terms of the T License (**value “No” for column “R License Compatible with T License”**), **go to Step 7.**

### **Step 7**

If the value of column Relation **is I**, **go to Step 10.**

If the value of column Relation **is C**, **go to Step 8.**

### **Step 8**

Fill in column “Linking R License”.

If the R License allows linking at compilation time and/or runtime (depending on which is the case) from software released under the T License add value “Yes” in column “Linking R License”.

If the R License does not allow linking at compilation time and/or runtime (depending on which is the case) from software released under the T License add value “No” in column “Linking R License”),

Then **go to Step 9.**

### **Step 9**

If the R License allows linking at compilation time and/or runtime (depending on which is the case) from software released under the T License (**value “Yes” in column “Linking R License”**), **go to Phase B** (Phase A is concluded positively).

If the R License does not allow linking at compilation time and/or runtime (depending on which is the case) from software released under the T License (**value “No” in column “Linking R License”**), **go to step 10.**

### **Step 10**

Fill in column “R License Exception”.

If the Reused is released by the licensor(s) with an exception that allows (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License add value “Yes” in column “R License Exception”).

If the R License does not allow (i) making a modified version with and/or (ii) linking at compilation time and/or runtime from (depending on which is the case) software released under the T License add value “No” in column “Linking R License”.

Then **go to Step 11.**

## Step 11

If the Reused is released by the licensor(s) with an exception that allows (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License (**value “Yes” in column “R License Exception”**), **go to Phase B** (Phase A is concluded positively).

If the R License does not allow (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License (**value “No” in column “Linking R License”**), **the compatibility test is not passed.**

## Phase B

Phase B is performed if Phase A is concluded positively.

Phase B verifies **if the T License allows licensing the Target including the Reused.**

### Step 12

Fill in column “T License Copyleft”.

If the T License is a copyleft license add value “Yes” in column “T License Copyleft”.

If the T License is not a copyleft license add value “No” in column “T License Copyleft”.

Then **go the step 13.**

### Step 13

If the T License is not a copyleft license (**value “No” for column “T License Copyleft”**), **the compatibility test is passed.**

If the T License is a copyleft license (**value “Yes” for column “T License copyleft”**), **go to Step 14.**

### Step 14

Fill in column “T License compatible with R License”.

If the T License allows including in the Target the Reused under the terms of the R license add value “Yes” for column “T License Compatible with R License”.

If the T License does not allow including in the Target the Reused under the terms of the R license add value “No” for column “T License Compatible with R License”.

Then **go to Step 15.**

### Step 15

If the T License allows including in the Target the Reused under the terms of the R license (**value “Yes” for column “T License Compatible with R License”**), **the compatibility test is passed.**

If the T License does not allow including in the Target the Reused under the terms of the R license (**value “No” for column “T License Compatible with R License”**), **go to Step 16.**

### **Step 16**

If the value of column Relation **is I**, **go to step 19.**

If the value of column Relation **is C**, **go to Step 17.**

### **Step 17**

Fill in column “Linking T License”.

If the T License allows linking at compilation time and/or runtime (depending on which is the case) to software released under the R License add **value “Yes” in column “Linking T License”**.

If the T License does not allow linking at compilation time and/or runtime (depending on which is the case) to software released under the R License add **value “No” in column “Linking T License”**.

Then **go to step 18**

### **Step 18**

If the T License allows linking at compilation time and/or runtime (depending on which is the case) to software released under the R License (**value “Yes” in column “Linking T License”**), **the compatibility test is passed.**

If the T License does not allow linking at compilation time and/or runtime (depending on which is the case) to software released under the R License (**value “No” in column “Linking T License”**), **go to step 19.**

### **Step 19**

Fill in column “Exception for T License”.

If the R License allows (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception add value “Yes” in column “Exception for T License”).

If the R License does not allow (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception add value “No” in column “Exception for T License”.

Then **go to Step 20**.

### **Step 20**

If the R License allows (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception (**value “Yes” in column “Exception for T License”**), **go to step 21**.

If the R License does not allow (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception (**value “No” in column “Exception for T License”**), **the compatibility test is not passed**.

### **Step 21**

Fill in column “Exception for other Reused”.

If the licenses of all Reused allow (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception add value “Yes” in column “Exception for other Reused”.

If the licenses of all other Reused do not allow (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception add value “No” in column “Exception for other Reused”.

Then **go to Step 22**.

### **Step 22**

If the licenses of all Reused allow (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception (**value “Yes” in column “Exception for other Reused”**), **the compatibility test is passed (but an exception has to be added to T License)**.

If the licenses of all other Reused do not allow (i) making a modified version with software and/or (ii) linking at compilation time and/or runtime from software (depending on which is the case) released under the T License with an exception (value “No” in column “Exception for other Reused”), **the compatibility test is not passed**.

# Annex C: Digital Data Commons Privacy Pledge

This Annex offers the Digital **Data Commons Privacy Pledge** to be undertaken by the User Data Recipient in order to access datasets including personal data.

The Digital **Data Commons Privacy Pledge** provides a set of commitments that can strengthen the powers of the data subject as set up by the EU GDPR.

## Digital Data Commons Privacy Pledge

### 1. Definitions

For the purposes of this Digital Data Commons Privacy Pledge (hereinafter “**Pledge**”), the following definitions apply.

“**Data**”: the personal data indicated in the Information.

“**Dataset**”: the dataset of the Promisor including the Data.

“**Group of Data Subjects**”: all the data subjects to which the personal data included in the Dataset are referred.

“**GDPR**”: the 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).

“**Information**”: the text, to which this Pledge is attached, including the information provided by the Promisor to the Promisee according to Article 13 or Article 14 of GDPR at the time when the Data are obtained.

“**Process**”: the act of processing.

“**Promisee**”: the data subject provided with the Information and this Pledge.

“**Promisor**”: the person or entity undertaking the Pledge.

“**Safe Place**”: the territory of Member States within the European Union whose laws (i) provide that its intelligence services are subject to adequate judicial and/or parliamentary control mechanisms; (ii) do not allow public authorities to perform mass surveillance practices, and/or the creation of “back doors” or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses; (iii) only allow public authorities to process personal data for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity, and (iv) effectively comply with the Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

“**Unsafe Place**”: the territory of Countries that cannot be considered Safe Place and international organisations.

All the definitions set by Article 4 of the GDPR apply, such as **personal data**”, “**data subject**”, “**processing**”, “**controller**”, “**processor**”, “**third party**” and “**consent**”.

## **2. Promise to respect privacy**

The Promisor irrevocably promises to process the Data complying with the GDPR, other applicable laws, and the provisions of this Pledge.

## **3. Data deletion**

The Promisor promises to **delete** the Data at the end of the period indicated in the Information, waiving the right to process the Data for any further period of time eventually allowed by applicable laws, except for the case the Promisee gives her consent.

## **4. No further purposes**

The Promisor promises to process the Data exclusively for the **purposes** expressly indicated in the Information, waiving the right to any processing for further purposes eventually allowed by applicable laws, except for the case the Promisee gives her consent.

## **5. List of processors**

The Promisor promises to process the Data using exclusively processors that are expressly indicated, with their details, in the Information, waiving the right to use any further processor eventually allowed by applicable laws, except for the case the Promisee gives her consent.

## **6. No Unsafe Place**

The Promisor promises to store the Data in a Safe Place and to **store or transfer** the Data to an Unsafe Place only if the Promisee gives her consent, waiving the right to any further transfer eventually allowed by applicable laws.

## **7. Notice of disclosure**

If the Promisor is legally requested to disclose the Data by any authority, the Promisor shall promptly provide the Promisee with a written notice so that the Promisee may seek for a protective order or other appropriate remedy.

## **8. Jurisdiction**

The Promisor promises to submit to the exclusive **jurisdiction** of the courts of any and all of the EU Member States selected by the Promisee.

## 9. Right to claim for the Group of Data Subjects

The Promisor allows each and all the members of the Group of Data Subjects to **claim rights for** and on behalf of **all** the other members of the Group of Data Subjects.

## 10. Research for the Common Good

If the Promisor performs research activity and the purposes indicated in the Information include the processing of the Data for research purposes, the Promisor promises that each and all the **results** of the research activity will be **made publicly available as open** as possible, in an effective way, including the adoption of licenses that allow the use, study, modification and distribution, including in modified form, of the results of the research activity.

## 11. Personal use exception

Notwithstanding any other provision of this Pledge, if the Promisor is a human being, he is allowed to process the Data in the course of a purely personal or household activity.

## 12. Miscellaneous

It is Promisor's intent that the Pledge be legally binding, irrevocable and enforceable against the Promisor and entities controlled by the Promisor, and their successors and assigns.

The Promisor will require any person or entity to whom it transfers the Data (third parties to which the data is disclosed and processors that the Promisor will use to process the Data) to agree to abide by the Pledge and to require any subsequent transferees to do the same.

In case of conflict between the commitments of this Pledge and the non-mandatory provisions of the GDPR and/or other applicable laws, the commitments of this Pledge shall prevail.

The above provision and each and all the obligations provided by the Pledge apply to the maximum extent permitted by applicable laws.