SPARTA

D10.3

Project results description documentation

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D10.3/ V1.0
Work package contributing to the deliverable	WP10
Due date	January 2020 – M12
Actual submission date	7th February, 2020

Responsible organisation	SMILE
Editor	Bertrand Lathoud
Dissemination level	PU
Revision	V1.0

Abstract	This document provides documentation and templates necessary for the identification and documentation of the produced resources.
Keywords	Identification of assets Documentation of assets Templates Assessments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Bertrand Lathoud (SMILE)

Contributors (ordered according to beneficiary numbers)

Elena Kaiser (SMILE)

Tun Hirt (SMILE)

Reviewers (ordered according to beneficiary numbers)

Thibaud Antignac, Augustin Lemesle (CEA)

Dirk Kuhlmann (FHG)

Mauro Gil Cabeza (IND)

Disclaimer

Executive Summary

D10.3 consists of a set of templates, guidelines and assisting documentation for adequately identifying and documenting the results produced by SPARTA's research programs. Further to addressing generic issues that must be dealt with independent of the nature of a research project, SMILE investigated aspects of identifying intended outcome and how to prepare for their documentation. The objective of this deliverable is to maximize SPARTA's chances to implement a sustainable exploitation plan, but also to support the EU wide aim of creating widely shared scientific knowledge and foster open science.

For both Intellectual Property and Privacy, two types of content are provided: documentation for helping to understand the nature of the legal issues, guidelines and templates for supporting the programs in dealing with them. We also designed a generic process dealing with the practicalities of documenting and securing assets which a strong view on efficiency.

It is included documentation for handling generic legal issues, and guidance for decision making on topics like ownership of results. This enables participants of SPARTA's program to identify and to document results of their work by following a simple and standardized process, and to re-use outcomes of previous activities. It has been developed guidelines for ensuring the security of results that can be applied when an update of the Data Management Plan or assessment of pre-existing resources is required.

Table of Content

List of Figures

Chapter 1 Introduction

The aim of the SPARTA project is to establish and operate a pilot for an EU Cybersecurity Competence Network. Strongly guided by strategic opportunities, impactful challenges, and measurable progress metrics, it will set up unique collaboration means, leading the way in developing and implementing a common cybersecurity research and innovation roadmap, building transformative capabilities and forming world-leading expertise centres. The SPARTA network implements research and innovation Programs, with a mission to support the development of transformative capacities in the field of cybersecurity and to supply technical means to the European industry to ensure its cyber-protection.

In order to achieve these goals, the SPARTA Consortium partners shall engage in the definition of a sustainable exploitation model for each of the research projects' outcomes. This involves a careful management of the resources used to conduct the research activities and of the resources produced due to requirements in particular.

After having identified and assessed the pre-existing resources (Deliverable D10.1) and created a Data Management Plan (DMP – Deliverable D.10.2) in previous steps, the next logical step is to assess the so far produced resources as the programs are generating their first results. Thus, the goal of this deliverable is to allow the identification and the documentation of the produced resources, in order to facilitate their further dissemination and exploitation in a way that supports the EU objectives around the development of cybersecurity capacities.

The following principles should be respected in the identification process:

- Ensure a strong legal security for all assets needed for exploitation of SPARTA's project results or promoted solutions (platforms, software and/or methodologies);
- Set up a common exploitation strategy by providing necessary documents and resources in order to harmonize results exploitation;
- Ensure the sustainability of all software developments within the SPARTA project by providing legal support and information on exploitation of results both for internal and external consortium needs.

There are some challenges that will have to be overcome. As with the previous deliverables, the possible disconnection with the program level and the "meta-level" (WP10 and SPARTA governance), may generate some difficulties related to the standardization of the results of the identification as well as for the documentation of produced resources process.

Another difficulty may lie in the lack of necessary focus on exploitation. A more natural approach may indeed favour further research work than any other type of exploitation.

Finally, the possible volume of generated results, in particular if they consist of data, could also cause issues by limiting the ability of the individual programs to document these results properly, due to a lack of available resources to do so. Efficiency will therefore be of utmost importance for the creation of designing processes and guidelines regarding identification and documentation actions.

Based on the DMP and the APER provided by the project leaders during the previous phase, SMILE has produced a body of legal documentation. Its purpose is to provide support to the project partners during the following phases, in particular for creating a sustainable and lasting exploitation plan. It consists of templates and guidelines addressing the most risks and concerns most relevant for the development and exploitation of software and technical tools.

The majority of documented risks are related to:

- Infringement of third party's Intellectual Property rights;

- Protecting data from being stolen or copied by third parties, also resulting in IPA loss,
- Protecting personal data subjected to the GDPR.

Hence, the objective is to determine a secure and resilient solution that is compliant with the applicable international and European legal frameworks. In practical terms, it is suggested to proceed in three steps:

1. To explain the rationale supporting the process, and its positioning in the overall Sustainable Exploitation framework.
2. To describe in detail the Identification and Documentation of Produced Resources (IDPR) process.
3. To define specific guidelines for critical and generic issues such as privacy or security.

This stepwise process will be reflected by the structure of the documents.

Chapter 2 IDPR as Element of Sustainable Exploitation

2.1 Positioning and IDPR in a Sustainable Exploitation Framework

Identifying and retrieving relevant data is critical to the work of scientists and innovators, and the European Union wants to ensure that the outcome EU funded research is made available to the public as widely as possible. The Community Research and Development Information Service (CORDIS)[1] was one of the most prominent initiatives and continues to serve as a primary source of results from projects funded under the EU's framework programmes for research and innovation. It was succeeded by the Open Access Infrastructure for Research in Europe (OpenAIRE)[2].

Both enabled sharing the results of numerous research projects more widely. As highlighted by the report on the European Open Science Cloud (EOSC) strategic implementation plan[3], the annual increase in volume of data has reached a point where information is produced faster than can be read even in confined domains. In transdisciplinary research such as performed by SPARTA, this problem is even more pronounced. Given SPARTA's size and objectives, this pilot can serve as a use case for exploring how to best develop a suitable framework for the EC and European Research Council (ERC) objectives around open science. This solution should be sufficiently flexible for being replicated by other European initiatives and the National Cybersecurity Coordination Centres of the future.

To this end, we need a minimal set of meta-data for identifying and locating the outcomes of the research work. Since it is not an option to expose these assets until decisions on sustainable exploitation have been reached, we also need guidelines for immediate protection.

SPARTA's technical programs are expected to produce a significant number of artefacts, both of digital and analogical nature. These artefacts have to be identified in terms of resources produced in order to assess the range of exploitation options from different angles, to enable reusing them throughout the programs, and to ensure further exploitation beyond SPARTA.

As illustrated in the Figure below (Figure 1), produced resources that are neither digital nor data based have to be directly accounted for in the Exploitation Planning. For data-based outcomes, an update of the Data Management Plan (DMP) is required.

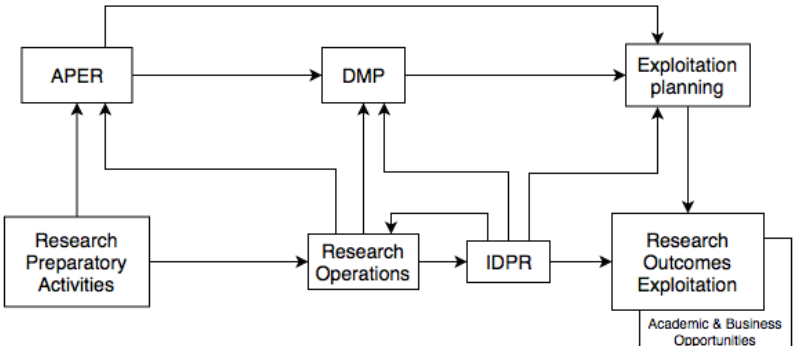


Figure 1: Position of the IDPR in the Exploitation Process

[1] Available at: https://cordis.europa.eu/about/en
[2] Available at : https://www.openaire.eu
[3] Available at : https://op.europa.eu/en/publication-detail/-/publication/78ae5276-ae8e-11e9-9d01-01aa75ed71a1/language-en

2.2 Process description and implementation challenges

In itself, the process is made of two phases, identification and documentation. However, it is important to highlight that identification in itself is part of the documentation process. We keep it separated for practical reasons, as it is self-contained and as it is the necessary step of the overall process. The further stages of the documentation process can indeed be skipped, even if this would have a detrimental effect on the planned exploitation of the results of the research activities.

Process description

Phase I: Identification

The focus lies on solving a single issue, i.e. to allow participants of the projects, and any other interested party, to get the necessary information for locating the assets and knowing about their nature.

Step 1: Name of the asset

To ensure consistence, a standard naming scheme should be followed. As it is not straightforward, more detailed information can be found in the next part, 3.2, on existing challenges.

Step 2: Nature

The nature of the assets can be Data, Documents, Software or Hardware (including infrastructure)

Step 3: Location

The location can be physical, or/and logical, in case the asset is not physical.

Phase II: Documentation

The documentation part shall provide insights about the intended usage of the asset, but also on several critical aspects such as its intended usage, its legal status, who owns it, what are the related security requirements and any scientific meta-information that would facilitate planning for further exploitation or dissemination action.

Furthermore, some of the most sensitive and generic issues have to be documented within in this phase. These are the privacy assessment of the resources if relevant, the legal issues around Intellectual Property, and finally the security requirements. All have to be carried out in any case in order to protect both the results and the researchers.

Step 1: Description of the possible usages and which ones were intended to be of higher priority
Step 2: Identification of ownership
Step 3: Documentation of the legal status
Step 4: Addition of required meta-data
Step 5: Documentation of specific issues: within this stage, the generic issues, i.e. privacy and security requirements, and Intellectual Property issues, have to be dealt with.

Implementation challenges

The first questions to be addressed are those of process ownership, responsibilities, and type of resources required for its implementation groups. The different stakeholders should decide the best course of action without harming the outcome of the process itself. These decisions should be documented.

A second set of questions concerns issues of local versus global orientation. Should the programs be completely autonomous to maintain maximum flexibility? Or should they have some degree of consistence with a global standard thereby furthering dissemination or sustainable exploitation, but at the cost of some overhead on the programs side?

The third major point regards the structure for handling the documentation, which is predicated on the type and magnitude of the produced results. Uncommon and non-standardized data formats should only be allowed if dictated by exceptional circumstances.

The structure of the directory will have a significant influence on the technology chosen to implement it. Those in charge of documenting research results are well advised to make efficient use of resources and to avoid giving preference to simple and sustainable solutions.

The most difficult decision concerns the level of standardization when naming the resources. Naming schemes are tricky as they are often result of non-explicit choices, such as local culture or habits. Preference should be given to a simple standard that provides flexibility through the use of keywords, but is sufficiently consistent to support rapid identification of the named resources.

Proposed Naming Scheme

X.UN_TYPE_DATE_VER_Keywords

- X = Program ID
  - 4
  - 5
  - 6
  - 7
- TYPE
  - DOC
    - Documents or data
  - DEV
    - Device, which can be any type of physical system
  - SOF
    - Software
- VER
  - Version
    - tt.uu : always two figures => 0 is explicit.
- Keywords
  - These should help to identify the asset, in the most efficient way, which means the least amount of words for the highest “quantity” of information about the asset. They may include names of authors, organizations, etc.

The last point to be taken care of is the question of metadata. Although it is still possible to create a tailored taxonomy that would fit exactly what the research programs are considering as significant meta-data for their dissemination and sustainable exploitation efforts, it is preferable to rely on a disciplined implementation of specific standards in order to prevent ambiguous definitions that would harm further scientific collaboration.

In case of generation of such local taxonomies, it is preferable to invest some time and resources in defining a correspondence with an existing standard. A source of documentation on existing standards can be found on the site of the Metadata Standards Directory Working Group.[4]

[4] Available at: http://rd-alliance.github.io/metadata-directory/

Chapter 3 Assessment of Privacy related risks

In order to create a sustainable and lasting exploitation plan for the project outcomes, an assessment of privacy related risks and the creation of an exhaustive and complete strategy about the treatment of personal data are of utmost importance.

The entry into force of the Regulation 2016/679 (GDPR) has reinforced the right to privacy in all Europe. Notwithstanding that, for many companies, compliance with the GDPR is still a challenge. For this reason, the documents presented in the next pages will support, first project partners, and the afterward eventually external organizations, to identify legal obligations imposed by the international and European legal framework when processing personal data.

The approach on this topic is mostly practical, i.e. based on potential risks for compliance related to the personal data processing and, in the meantime, the documentation will help the data controller to create his own processing scheme.

The following chapters will first introduce the legal framework of data protection on both a European and International level, then provide a flowchart intended to give a detailed overview of all possible impact, the GDPR can have on a data processor or controller. The last chapter provides a template dedicated to create a privacy risk assessment for every processing of personal data within the project.

All this activity is relevant both from a legal/compliance perspective and ethical one.

3.1 Data protection principles and legal framework

3.1.1 International level

At an international level, the right to privacy is protected by article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.

Article 12 (Universal Declaration of Human Rights): “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”.

Article 17 (International Covenant on Civil and Political Rights): “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation”.

As it might be noticed, the content of these two provisions is quite similar and they differentiate from each other only for the fact that the Universal Declaration of Human Rights, being a so called soft law source, does not have binding effects. On the contrary, the International Covenant is an international treaty and its respect by Member states is monitored by the Human Rights Committee.

However, none of the text contains any explicit reference to the right for the protection of personal data. This lack in the law is mostly due to the historical circumstances, being the Universal Declaration of Human Rights been dated to 1948 and International Covenant on Civil and Political Rights to 1966, when technology was not advanced in the data science field.

The concept of personal data entered the international legal framework only with the Council of Europe Convention 108/1980. This latest is considered, until now, the first and the only international Convention on data protection.

Actually a year before, in 1980, the Organization for Economic Cooperation and Development (OECD) published the Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data[5] but this document, as the name "guidelines" suggests, does not have binding effects.

The same can be said for the Guidelines for the Regulation of Computerized Personal Data Files, published by the General Assembly of the United Nations on the 14th of December 1990. However, these two documents, although not legally binding, played an important role in the development of the subsequent framework of data protection.

Going back to the Convention of the Council of Europe, the first version of this document was adopted on the 28th of January 1981 The Convention for the Protection of Individuals with regard to Automatic Processing of personal data. The treaty acknowledged the need for a stronger protection of personal data, also with regard to the increase of international flow of them in an automatic manner.

The most important principles established in the Convention were:

Quality of data (article 5): personal data undergoing automatic processing shall be obtained and processed fairly and lawfully;

- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date;
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

***Ad hoc* rules for special categories of data** (article 6)

Data security (article 7);

Transparency (article 8): right to obtain confirmation of whether personal data relating to her/him are stored in the automated data file as well as communication to her/him of such data in an intelligible form;

Right to rectification and erasure (article 8, c)

A new amended version of the Convention was adopted on the 18th of May 2018, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, or also simply called Convention 108+. The main novelties are represented by:

- The reinforcement of the principle of **transparency** (article 8): data subjects have granted new rights that allow them to have a greater control (article 9) over their data, in particular for the information that has to be communicated when exercising their right to access;
- Principle of **proportionality** (article 5);
- Principle of **accountability** (article 10);

Data minimization (article 5),

Privacy by design (article 10)

Data breach (article 7): the requirement to notify is limited to cases which may seriously interfere with the rights and fundamental freedoms of data subjects, which should be notified, at least, to the supervisory authorities.

3.1.2 European Level

[5] Organisation for Economic Coperation and Development (OECD), *Recommendation of the Council concerning guidelines governing the Protection of Privacy and Transborder Flows of Personal data*, 23th. September 1980.

The European institutions of the then European Community started to gain interest on data protecting issues in the 1980s, when the European Commission urgently recommended Member States to ratify Convention 108 of the Council of Europe, in order to harmonize national regulations and promote a common market in the information field.

Today, personal data are primarily protected in the European Union treaties. Indeed, the Treaty of Amsterdam of 1997 provided, in Article 286 TEC, paragraph 1, that "From 1 January 1999 the Community acts on the protection of natural persons with regard to the processing of personal data as well as the free circulation of such data applies to the institutions and bodies established by this treaty or on the basis of the same".

But it is finally with the Treaty of Lisbon that the protection of personal data has been recognized as a fundamental principle of the European Union. The European Union has in fact, through Article 16 TFEU (formerly Article 286 TEC), the specific competence to protect, through ordinary legislative acts subject to the control of independent authorities, personal data of the individuals. For the protection of the aforementioned rights, the European Union may also appeal, if necessary, to the Court of Justice.

In fact, article 8 of the Charter of Fundamental Rights has now, due to the provision contained in the new article 6, c. 1, TEU, the same legal value as the Treaties. In particular, article 8 establishes that:

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority".

The right to privacy is also protected by 8 European Convention of Human Rights:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Regarding this article, there is a lack of any explicit reference to the personal data. The inclusion of this latest concept into article 8 ECHR constitutes the result of the jurisprudential evolution of the European Court of Human Rights on this subject, which began with the case Klass and others v. Germany.[6] However, the European Convention of Human Rights is not part of the European Union system but of the Council of Europe one - a international human rights organization founded in 1949 and formed by 47 States, among which the 28 EU Member States. Even though the Convention is not part of the European Union, article 8 ECHR has an important impact on role in the national and European jurisprudence on data protection.

Regarding the European secondary legislation (*i.e*. regulations, directives, decisions, recommendations and opinions), the first and most important reference text concerning the protection of personal has been for years the directive 95/45/EC, now replaced by the Regulation (EU) 2016/679 (GDPR). Additionally, it can be found the directive 2002/58, the so called e-privacy directive, and the regulation 2018/1725 concerning the protection of natural persons in relation to the processing of personal data by the institutions and the community bodies, as well as the free circulation of such data and the directive 2006/24/ EC.

Still in this context, stands out for its importance the Council Framework Decision 2008/977 of November 27, 2008 on the protection of personal data processed in the framework of police and

[6] European Court of Human Rights (Plenary), *Klass and others v. Germany*, 6th. of September 1978, application no. n. 5029/1971.

judicial cooperation in criminal matters, now replaced by the Directive (EU) 2016/680 and, finally, Directive 2009/136 / EC "amending the 2002/22 / EC directive on universal service and users' rights in the field of electronic communications networks and services".

Finally, it has be mentioned that the directive 2016/1148 on security of network and information systems (the so called NIS directive), refers to personal data as compromised result of incidents. According to the new Cybersecurity Act[7] that entered into force in 2019, one of ENISA's task (European Network and Information Security Agency) is to support "Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to *data protection* and *privacy*"[8].

3.1.3 Data protection principles

However, the regulation that is mostly impacting companies' activities in this moment is for sure the GDPR. This latest has, in fact, introduced many important novelties in comparison to the previous directive on data protection, such as its extraterritorial application under Article 3, the concepts of privacy by design and privacy by default, or the right to data portability. All these rights will, from one side, enhance and reinforce the rights of individuals but, from the other side, impose new requirements for organisations when processing personal data.

As general principles, according to article 5 GDPR, every processing of personal data should be:

a. **lawfulness, fairness and transparency;**
b. **purpose limitation;**
c. **data minimization;**
d. **accuracy;**
e. **storage limitation;**
f. **integrity and confidentiality.**
g. **accountability.**

The data processing is considered **lawful** if taking place in respect of the following conditions (article 6 GDPR):

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- 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;
- processing is necessary for **compliance with a legal obligation** to which the controller is subject;
- processing is necessary in order to **protect the vital interests of the data subject** or of another natural person;
- 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;
- 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.

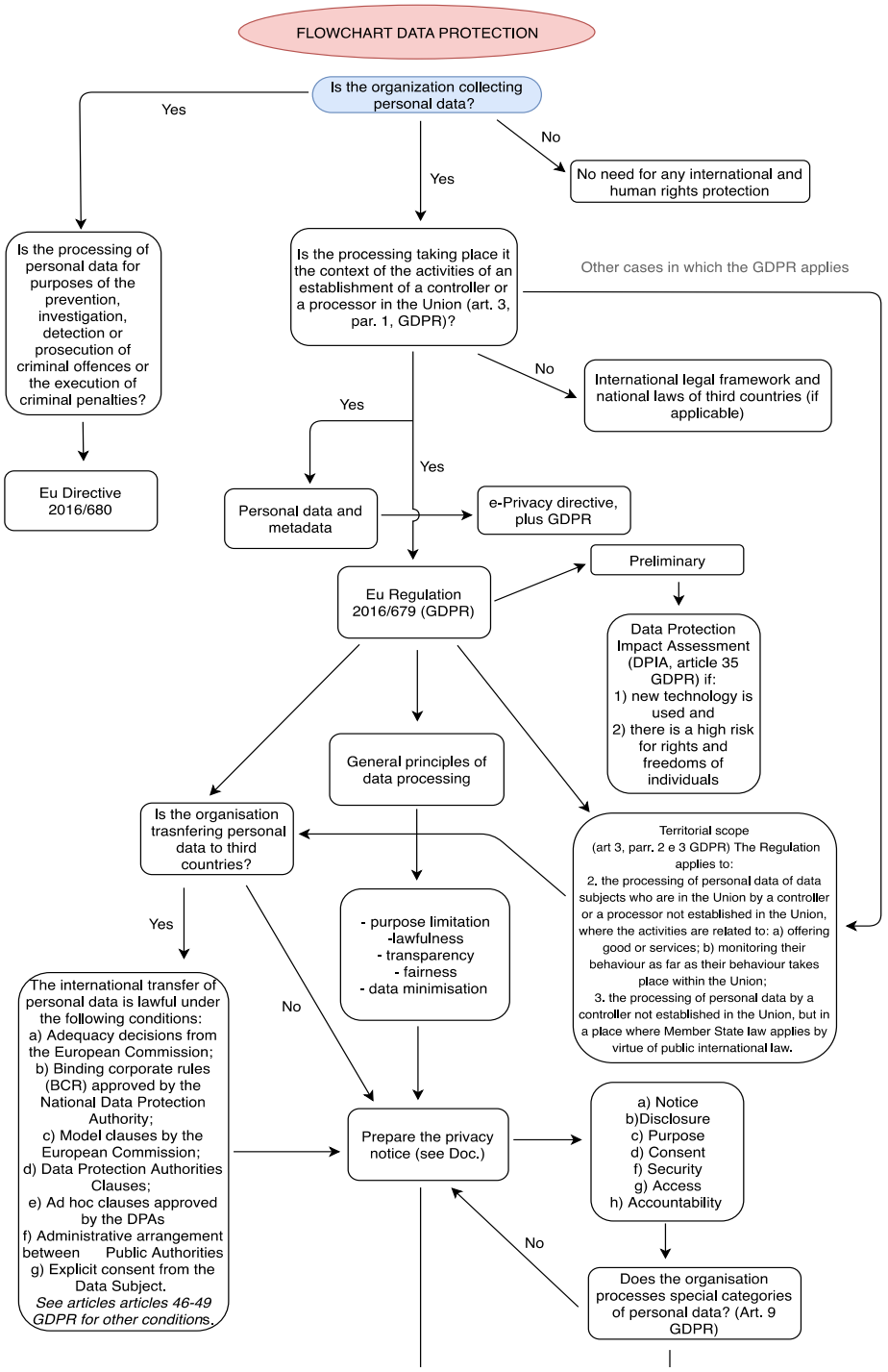
Another important principle of the GDPR is **Security**. Indeed, according to article 21 of the regulation the data controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

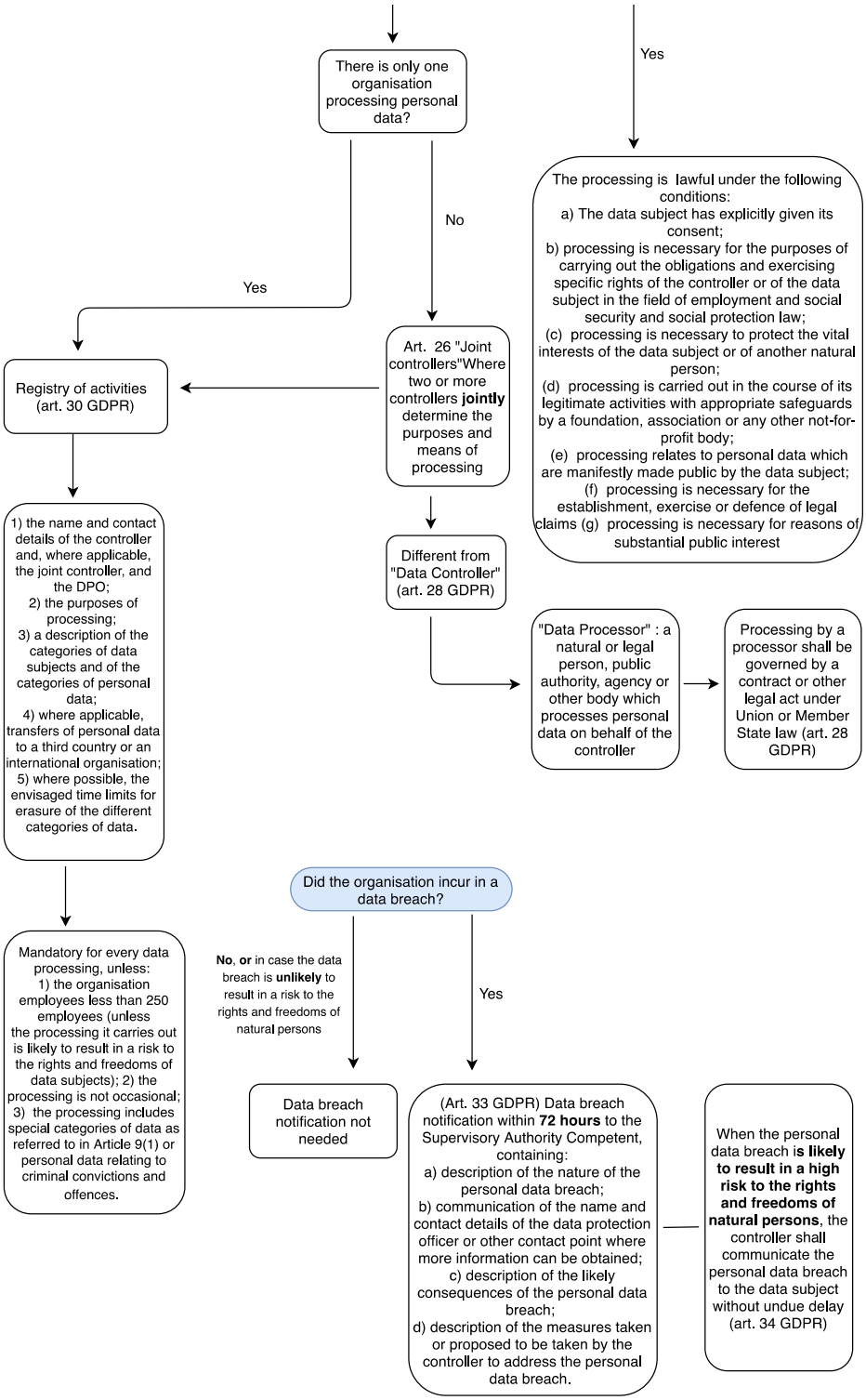
[7] Regulation (eu) 2019/881 of the European parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[8] Article 5 Cybersecurity Act.

a) the **pseudonymization** and **encryption** of personal data;
b) the ability to ensure the ongoing **confidentiality, integrity, availability** and **resilience** of processing systems and services;
c) the ability to **restore** the **availability** and **access** to personal data in a timely manner in the event of a physical or technical incident;
d) a process for **regularly testing**, **assessing** and **evaluating the effectiveness of** technical and organizational **measures** for ensuring the security of the processing.

3.2 Data protection flowchart

The following flowchart shall provide an overview as well as decision-making support for the European legal framework related to the protection of personal data, in particular the GDPR. The flowchart addresses to any kind of organization processing personal data and at first identifies the main obligations under the GPDR and secondly identifies what to do in case of a data breach as well as potential sanctions in case of non-compliance to the GDPR.


FLOWCHART DATA PROTECTION
Is the organization collecting personal data?
Yes
No
No need for any international and human rights protection
Yes
Is the processing of personal data for purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties?
Is the processing taking place it the context of the activities of an establishment of a controller or a processor in the Union (art. 3, par. 1, GDPR)?
Other cases in which the GDPR applies
No
International legal framework and national laws of third countries (if applicable)
Yes
Eu Directive 2016/680
Yes
Personal data and metadata
e-Privacy directive, plus GDPR
Eu Regulation 2016/679 (GDPR)
Preliminary
Data Protection Impact Assessment (DPIA, article 35 GDPR) if:
1) new technology is used and
2) there is a high risk for rights and freedoms of individuals
General principles of data processing
Is the organisation trasnfering personal data to third countries?
Territorial scope
(art 3, parr. 2 e 3 GDPR) The Regulation applies to:
2. the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union, where the activities are related to: a) offering good or services; b) monitoring their behaviour as far as their behaviour takes place within the Union;
3. 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.
Yes
- purpose limitation
-lawfulness
- transparency
- fairness
- data minimisation
No
The international transfer of personal data is lawful under the following conditions:
a) Adequacy decisions from the European Commission;
b) Binding corporate rules (BCR) approved by the National Data Protection Authority;
c) Model clauses by the European Commission;
d) Data Protection Authorities Clauses;
e) Ad hoc clauses approved by the DPAs
f) Administrative arrangement between Public Authorities
g) Explicit consent from the Data Subject.
See articles articles 46-49 GDPR for other conditions.
Prepare the privacy notice (see Doc.)
a) Notice
b)Disclosure
c) Purpose
d) Consent
f) Security
g) Access
h) Accountability
No
Does the organisation processes special categories of personal data? (Art. 9 GDPR)


There is only one organisation processing personal data?
Yes
No
Yes
The processing is lawful under the following conditions:
a) The data subject has explicitly given its consent;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims (g) processing is necessary for reasons of substantial public interest
Art. 26 "Joint controllers"Where two or more controllers jointly determine the purposes and means of processing
Registry of activities (art. 30 GDPR)
1) the name and contact details of the controller and, where applicable, the joint controller, and the DPO;
2) the purposes of processing;
3) a description of the categories of data subjects and of the categories of personal data;
4) where applicable, transfers of personal data to a third country or an international organisation;
5) where possible, the envisaged time limits for erasure of the different categories of data.
Different from "Data Controller" (art. 28 GDPR)
"Data Processor" : a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Processing by a processor shall be governed by a contract or other legal act under Union or Member State law (art. 28 GDPR)
Did the organisation incur in a data breach?
No, or in case the data breach is unlikely to result in a risk to the rights and freedoms of natural persons
Yes
Mandatory for every data processing, unless:
1) the organisation employees less than 250 employees (unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects); 2) the processing is not occasional; 3) the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences.
Data breach notification not needed
(Art. 33 GDPR) Data breach notification within 72 hours to the Supervisory Authority Competent, containing:
a) description of the nature of the personal data breach;
b) communication of the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) description of the likely consequences of the personal data breach;
d) description of the measures taken or proposed to be taken by the controller to address the personal data breach.
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay (art. 34 GDPR)

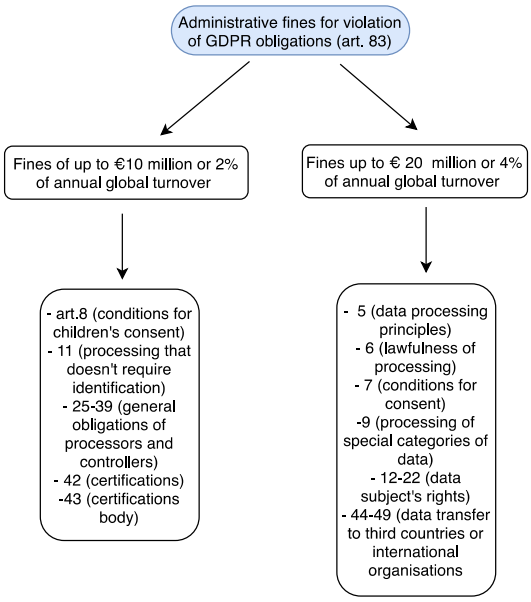


Figure 2: Data protection flow

3.3 Privacy Risk Assessment Template

The aim is to identify and assess the potential harm for individual data protection rights and the risks for a lack of compliance by the data processor.

This template shall identify if the GDPR requirements have been undertaken so far.

Each of the following issues should be address with a level of detail appropriate to the project. The template has to be fulfilled for every processing of personal data.

---

a. Are personal data involved in the processing? Indicate the type of data, the purpose of processing, adequacy, relevance and security requirements (see article 5 GDPR requirements), defined period of storage)

b. Lawfulness of the processing:

i. consent of the data subject (see conditions for the consent under article 7 GDPR);
ii. processing is necessary for the performance of a contract;
iii. processing is necessary for compliance with a legal obligation of the data controllers;
iv. processing is necessary to protect the vital interests of the data subject;
v. processing is necessary for the purposes of legitimate interests pursued by the data controller (see other requirements under article 6 GDPR)

c. Are special categories of data involved in the processing? See requirements under article 9 GDPR.

d. Information that has to be provided to the data subject when collecting personal information: see articles 13-20 GDPR for the requirements

e. Privacy by design and privacy by default measures: see article 25 GDPR

f. Joint controllers (if applicable): see definition and requirements under article 26 GDPR

g. Processor (if applicable): see definitions and conditions under article 28 GDPR

h. Records of processing activities (if applicable): see requirements under article 30 GDPR

i. Notification of a personal data breach: see conditions and requirements under articles 33 and 34 GDPR

j. There is a need of a Data protection impact assessment? See requirements under article 35 GDPR

k. Designation of a data protection officer (if applicable): articles 37, 38, 39 GDPR

l. Are personal data transferred to third countries? See conditions under articles 44-49 GDPR

m. There is any risk that the processing may violate one of the requirements of the GDPR indicated in article 83?

Chapter 4 Assessment of Security related issues

As part of the proper management of the data and information produced by the research program, protecting them from theft, manipulation or undue processing is required, whatever their usage in further exploitation phases will be.

Securing data and information requires first to know of the risks the assets are exposed to. It means then to formalise the principles and rules that will constrain storage, access and usage of these assets, depending on their exposure and needs of the users.

Given the transitory nature of the work package, it seems difficult to engage in the creation of a comprehensive Information Security Management System (ISMS). This would consume an inordinate amount of resources and time, and would therefore impact the ability of the Programs to deliver actual scientific results.

It makes more sense to perform a high-level risk assessment and focus on the development of rules and procedures for the most critical risks. Documenting the less significant ones may however be useful as part of the sustainable exploitation plan as it will make it easier for future owners of the produced results to handle them efficiently.

We suggest a set of guidelines for the generation of a simplified security policy through a three steps process:

1. Risk assessment
2. Definition of a security policy for the most critical assets and dealing with the most significant risks

Maintenance and update of the security policy depending on the progress of the research work, but also the definition of the sustainable exploitation plan, which may impact the way the assets and risks are assessed.

4.1 Preliminary risk assessment

Several methodologies do exist and the most widely used relies on the set of ISO 2700X standards aimed at creating a comprehensive ISMS. However, and in order to avoid consuming an excessive amount of resources, we'll rely on a simplified approach based on the MONARC methodology. It is both compatible with the ISO27005 standard, but also with the EBIOS assessment framework. It is as well licensed as Open Source and an Open Source tool, of the same name, is provided with its documentation[9].

The risk assessment follows four steps summarized below

1. Context documentation
   - **a.** Definition of the target of the risk analysis
     These will be the produced resources and related documentation. It may go further but this is not really required in the initial assessment.
   - **b.** Description of the context
     - Which processes will use or consume the assets?
     - What is the sensitiveness of the assets for the processes that use them?
     - Are there known legal or regulatory obligations?

[9] https://www.monarc.lu/

- Are there security needs already expressed around confidentiality, integrity of the assets, or availability?
- Are there any other requirements that would have been expressed by the stakeholders and that would impact the sensitiveness or the exposure of the assets?

c. Definition of the risk analysis criteria
- Damage assessment criteria: they should allow to define how to express the degree of damage and the associated costs, how to express damage in terms of reputation or damage caused by legal consequences.
- Qualitative or/and a quantitative scale: does the organisation want to work on a purely quantitative scale (estimating the different values on a quantitative scale, i.e. low to very high for example, or 1 to 5), and does it want to have also a quantitative approach, keeping in mind that the latter is extremely cumbersome to set and manage, and may not provide much more in terms of precision or relevance of the risk analysis.
- Risk acceptance criteria: needed to define acceptable levels of risk (potentially different for confidentiality, integrity and availability)
- Scope of the risk analysis: what are the criteria allowing to decide if an asset is within or outside the scope of the risk assessment?
- Other decisive criteria such as the organisation's values, and in particular ethical concerns

d. Structure of the risk approach
- Description of the risk management process
- Definition of actors and their respective roles in the risk management process
- Documentation of escalation mechanisms
- Description of the relationships between risk assessment operators and stakeholders
- List of records that need to be kept and are used to document the risk management process
- Documentation of the choice of methodology

2. Context modelling

Development phase of the risk model focused on the primary assets to be protected. It consists in creating dependency trees between the various assets and to be able to formally describe:

a. The assets themselves with a focus on their relationships
b. The classification rules for the assets
c. The threats that are relevant for such assets
d. The vulnerabilities related to these assets
e. The existing security controls
f. The possible impacts

3. Risk evaluation and controls' design

a. Setting the level of threats and vulnerabilities of the context type under review.
b. Computing the risk level
- estimation of the impacts
- estimation of likelihood of occurrence
- estimation of the risk level

c. Proposing security measures aimed at lowering major risks to acceptable levels and to accept low risks.
- For each risk, definition of a risk treatment among
  - "Risk reduction", which consists of reducing the risk by choosing the appropriate security objectives and measures (See: Sectoral risk analysis – risk treatment);

- "Risk retention", which consists of accepting current risks without taking further action;
- "Risk refusal", which consists of giving up the activity or domain at the source of the risk;
- "Risk transfer" to a third party, by means of insurance coverage, for example.

4. Controls implementation and continuous monitoring
    a. Implementation of the security controls

Assessment of the major changes to the risk analysis context on a regular basis, as well as any major changes beyond the initial context which would necessitate a new analysis iteration.

4.2 Definition of the security policy targeted at the most critical assets and for the most significant risks

The security policy shall formalize and coordinate all organizational and technical security procedures of the organization.

The objectives of the creation of a security policy are mostly:

1. To understand the requirements related to the security of the company's information and the necessity of introducing a security policy and objectives;
2. To implement and enforce security-related risk management measures in the context of the global risks related to the organisation's activity;
3. To monitor and continuously assess the Information Security Management System's (ISMS) performances;
4. Continuously upgrading the system based on objective measurements.

Writing a comprehensive and detailed security policy is a resource and time-consuming project.

Given the constraints of the programs, it would be problematic to engage in the design and implementation of a comprehensive ISMS. It's therefore recommended to start with a set of short documents focused on the most critical assets and describing the required security controls. These can be technical (tools and systems implementation and configuration) but also organisational (procedures and processes).

As they will be defined depending on their nature and on the preliminary risk assessment, it is not possible to provide a generic policy. It is however advised to rely on existing standards such as ISO 2700X (in particular ISO 27002 for the list of controls) or BSI Grundschutz[10]. MONARC itself provides a repository of common controls.

From the ISO 27002 suggested 11 domains of focus, it is at least possible to generate a few generic questions that will help to structure the documents to be created:

1. Information security policy
    a. Does the program have already formalised its security policy?
    b. If there is already a formal documentation related to the security of data or information assets, was it created following a specific methodology?
    c. If no standard or methodology was used, does the documentation cover all the relevant domains, as listed below, from organisation of information security to compliance?

[10] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

2. Organization of information security
    a. Is there a person in charge of the security policy design, implementation and maintenance?
    b. Is there at least a procedure for organising the maintenance and updates of the security policy?
3. Asset management
    a. Is the program managing its information related assets?
    It should be the case thanks to the work done for the Assessment of Pre-existing Resources (APER) and the Data Management Plan (DMP).
    b. Is there a procedure to update the assets management system?

4. Security related to human resources
    a. Are the persons who access the most critical data identified?
    b. If the risk assessments requires it, does a procedure exist to perform background checks before granting access to the most critical data?
    c. Is there a ruleset related to the change of status in the various partner organisations, that would allow to update their authorizations depending on the type of change that occurred

5. Physical and environmental security
    a. Is there a documented ruleset describing the way the systems handling the assets, in case of non-physical assets, or the assets themselves have to be protected regarding their physical manipulation

6. Use and management of communications
    a. Is there a documentation of the rules related to the usage of communications equipment, depending on the roles, locations, and types of assets?
    b. Are there preventive controls in place to enforce the rules?

7. Access control
    a. Is there a documentation of the generic roles that can access the assets and what type of access are they granted?
    This means that the time range of access, and the ability to process the assets should be clearly defined.
    b. Are there specific tools allowing to enforce the access controls ruleset?

8. Acquisition, development and maintenance of the information systems
    a. Are the procurement rules involving an analysis of the impact on security posture of the planned acquisition?

9. Incident management
    a. Is there a plan in place describing how to detect, investigate and resolve incidents?
    b. Are the possible mandatory reporting obligations documented?
    c. Are there members of the organisation that possess the necessary skills for implementing this plan? Are they informed of their role and have they been practicing the plan?

10. Business continuity management

a. Is there a plan to ensure a continuity of operations?
b. Is there a plan describing how to recover from an incident having rendered some or all of the assets unavailable.

11. Compliance
a. Is there a documentation of the generic regulatory and legal obligations applying to the assets and their usage?
The main focus should be on Privacy requirements, and also on respect and enforcement of Intellectual Property rights.

If relevant, are the specific regulatory requirements applying to the assets identified and documented? For example, are regulations on financial, health, or telecommunications sectors applying?

4.3 Maintenance and update of the security policy

As the security policy approach is initially lighter than suggested by more traditional methodologies and standards, it will require a more formal process for maintenance and update. If the initial documents are limited in number and depth, it is strongly advised to set a continuous improvement process consisting in gradually developing the policies both in scope and granularity.

This should be based both on timeframes, for example every six months, and on triggers such as specific events. One example being an update of the DMP due to the production of new datasets by the research program.

More generally, the progress of the research work, but also the definition of the sustainable exploitation plan may impact the way the assets and risks are assessed and must be taken into account as triggers for a possible update of the security policy.

A last point to be stressed is the importance of assessing which parts of the policy are not needed anymore. This is particularly sensitive for organisations with limited resources, in order to prevent an unnecessary use of resources for enforcing rules that are not useful anymore to the reduction or suppression of risk related to the most critical assets.

Chapter 5 Assessment of Intellectual Property related issues

The aim of this chapter is to provide the necessary information about the Intellectual Property protection of produced software assets. More precisely, the following chapters will focus on the produced software source code of the projects results. In this way, there will be first a detailed documentation on the use of source code audit, followed by a template that should be used to assess the undertaken steps regarding the preparatory and operational phases of source code audit regarding the concerned project results.

5.1 Legal Source Code Audit Guidelines

The aim of this documentation is to provide information about the use of legal source code audit. Source code audit is an important operation to be undertaken prior to the disclosure of software. Source code audit provides an overview of the Intellectual Property rights related to a software asset and increases, in the meantime, the value of it. This value increase is due to risk minimization, which leads to a stronger and more consistent business plan.

Legal source code audit is an operation by which a software developer ensures legal compliance regarding copyright and licensing issues of his source code.[11] There are, however, important steps that should be taken prior to the audit in order to reduce its size. These steps will be analysed in the first chapter, before dealing with the terms of the operation itself.

Indeed, including code audit is important to guarantee the achievement of the sustainable goals of the project's outcomes and more precisely the developed software assets. This documentation shall furthermore be considered as support to the creation of exploitation- and business models of the project.

5.1.1 Introduction

Legal source code audit is an operation by which legal and Intellectual Property compliance of a software source code is summarized, checked and verified.[12] Intellectual Property protection and compliance have to take an important place within the business plan of a company.

It is as well needed to ensure sustainability of product distribution. In both matters, protection and compliance, rather the company can incur severe economic losses through lack of protection or trough copyright infringement lawsuits.

Two main models of Intellectual Property in software licensing

Regarding Intellectual Property protection of software assets through licensing, there are two different models, the Open Source model and the so-called Proprietary model.[13] Technically, "Open

[11] European IPR Helpdesk, *IPR management in software development (p.12),* June 2013. Available at: https://iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-IPR-Management-in-Software-Development.pdf

[12] European IPR Helpdesk, *IPR management in software development (p.12),* June 2013. Available at: https://iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-IPR-Management-in-Software-Development.pdf

[13] Opensource.com, *What is Open Source.* Available at: https://opensource.com/resources/what-open-source

Source refers to software whose source code – the medium in which programmers create and modify software – is freely available on the internet. By contrast, the source code for proprietary commercial software is usually a closely guarded secret."[14] No matter under which model the software is released, Intellectual Property is present, and compliance is consequently required. As it got nearly impossible to write software code entirely from scratch, almost every software today contains code lines coming from Open Source.[15]

This document will explore different ways to combine effectivity and cost-efficiency of code review while highlighting its benefits. It will mainly focus on Open Source software. However, there are many similarities between the two different models and most of the operating methods related to code review can be applied to both. The document also contains a description of steps that can be taken prior to the actual audit in order to simplify the audit process itself.

Challenges in choosing the software license model

If software is distributed under the Proprietary model (or "closed source"), the source code is obfuscated and its re-usage or redistribution by third parties is prohibited. Essentially, ownership is not transmitted, and the software is distributed through licensing that only allows the users to use of the software. If software is published as Open Source, its source code is made available to everyone and the terms of re-usage and re-distribution depend on the type of license under which the software is released.

The choice between closed or Open Source determines the kind of property rights owned on the software market. It is as well important in the way that it has a substantial impact on the business-model and more generally, on the way a software is monetizable. Open Source however means in no way free, in the sense that such software would not be monetizable or could not create value.[16] Ownership may be transferred, but some Intellectual Property related rights remain either way in the portfolio of the developer. In addition, in most cases Open Source software is being monetized trough support, premium features or trademarks.

As it got nearly impossible to write a software code exclusively on an individual basis, software is nowadays mostly written, improved, enhanced and modified by a variable number of cooperating developers from different backgrounds. Furthermore, almost every released software product, closed or Open Source, contains Open Source based code lines.

According to Gartner research, as much as 95% of IT organizations leverage Open Source software within their mission-critical applications. [17] As it is much more efficient to use those freely available code lines rather than writing new ones, Open Source allows the whole developer community to work more efficiently, to freely collaborate, to be more interconnected and to be more sustainable in their work. This cooperative model increases the value of the products without requiring remuneration of the contributors.

Regarding Intellectual Property, software code is protected by copyright law as it is considered as "creative intellectual work" [18]. In this way, the copyright protection exists by default from the moment in which the code is written. However, in order to protect the software assets in a more efficient way,

[14] Dr. D. CROOKE, Open Source vs. Proprietary Software.
Available at: https://www.greennet.org.uk/support/open-source-vs-proprietary-software
[15] M. DRIVER, *Hype Cycle for Open-Source Software*, July 11, 2016.
Available at: https://www.gartner.com/en/documents/3371817/hype-cycle-for-open-source-software-2016
[16] M. WHEATLEY, *Red Hat posts solid Q2 earnings, subscription revenue grows,* September 21, 2016.
Available at: https://siliconangle.com/2016/09/21/red-hat-posts-solid-q2-earnings-subscription-revenue-grows/
[17] M. DRIVER, *Hype Cycle for Open-Source Software*, July 11, 2016.
Available at: https://www.gartner.com/en/documents/3371817/hype-cycle-for-open-source-software-2016.
[18] Berne Convention for the Protection of Literary and Artistic Works, latest Text of July 24, 1971.
Available at: https://global.oup.com/booksites/content/9780198259466/15550001

licensing should be used. Licensing is a legal tool that lays down the terms on which the copyright owner wants his software to be used by the users.[19]

There are very different ways to license an Open Source code. Redistribution can for example be allowed while imposing that the redistributor cannot change the license type itself. There are two main license schemes in Open Source, copyleft and permissive licenses.[20] Copyleft licenses do not allow to use the code and to integrate it into a closed source product. Permissive licenses on the other hand allow code integration into proprietary software and only require the used code to remain Open Source but not the software products build on top of or including this code. The main advantage of Open Source is that it strengthens innovative processes, increases product quality and security, while still being monetizable.

Overall benefits of source code audit

Code audit will in any way lead to a value increase of software assets and it is advisable to undertake it, no matter which distribution model, Open or closed source had been chosen. One reason to undertake an audit is to have a detailed overview about possible copyright infringement of the code.

However, in a more indirect way, this operation increases the value of intangible Intellectual Property software assets in the way that it shows a certain professionalism regarding the business strategy of a software publisher. By minimizing risks, essentially the risk to infringe those third party copyrights, potential burdensome lawsuits can be avoided.[21]

Regarding source code audit, specific software tools can operate an automated audit of the source code of a given software. The output of the audit-operation is an assessment of possible Intellectual Property rights infringement and security risks. The algorithms behind such tools identify correlations between code lines from the source code and code lines found in databases containing published and already licensed Open Source code. Based on the results, these tools are usually able to identify conflicting Open Source licenses as well.

The goal of legal audit is to minimize Intellectual Property infringement risks, avoid possible leaks of trade secrets, to summarize possible patent applications, to assure license compliance and to point out or suggest appropriate licenses for software products.[22] The use of the appropriate audit software may in this way solve several issues before they arise and before they can be harmful to a business.

5.1.2 Optimisation of the preparatory phase of the code audit

Nevertheless, before actually using an automated tool, some important steps have to be taken in advance. In terms of business efficiency, the sooner code compliance is taken into account within the development process, the less expensive the audit itself will be. In this way, a first step would be to train developers on "*license-awareness".* There should be specific procedures including regular reverse code check-ups as well as a proper documentation procedure of the code development (including summarization of all code under third party licences). Some tools assist with these tasks or simply automate them.[23]

---

[19] Techopedia Dictionary: Software Licensing Definition.
Available at: https://www.techopedia.com/definition/2558/software-licensing
[20] B. BYFIELD, *Open Source Debate: Copyleft vs. Permissive Licenses*, February 11, 2015.
Available at: https://www.datamation.com/open-source/open-source-debate-copyleft-vs.-permissive-licenses.html
[21] Active State, *License to Code: How to Mitigate Open Source License Risks*.
Available at : https://www.activestate.com/resources/white-papers/license-code-how-mitigate-open-source-license-risks/
[22] Open Logic, *Open Source Software Audits: Why, When, and How to Conduct an Audit,* April, 2011.
Available at: https://www.roguewave.com/sites/rw/files/documents/white-papers/openlogic-open-source-audits.pdf
[23] Education Ecosystem Blog, *10 Tools for the Perfect Code Documentation*, August 15, 2016.
Available at : https://blog.education-ecosystem.com/code-documentation-tools/

The creation of, and compliance to, these specific procedures both increase business-efficiency and have a serious impact on the value-increase of the produced code. In fact, a proper real-time documentation about the source-code is primordial in terms of cost-efficiency of the final code review. If the developers working on a code are trained on copyright-issues awareness, the audit process will be less extensive and less expensive in the same time. Thus, the better developers are prepared prior to the development of the source code, the less the code has to be modified afterwards, at least in terms of compliance.

Another issue is the organization of the source code structure itself. A software and its related source code is usually made up of a large number of single files gathered in a main directory. In order to make code review less extensive, a proper organization of this directory is of advantage.[24] The number of different languages used for documentation for example has an impact on the extent of the review as well.

It shall be noticed that each code is unique and that all indications given here are at most approximations. There are other factors like the complexity of the code, the efficiency, the structure of the software, the error quote, the pre-audits by the developers themselves and the resources of the reviewer company, that have to be taken into account.

The legal source code review before disclosure of the software is as well an investment in the way that it can prevent legal suits, which could be seriously harmful at a later stage. It clearly lays down the Intellectual Property infringement risks that may be faced after software disclosure. It is possible as well to combine the legal source code review with a security review. As those operations are in most cases today done in the same time, combing them enhances generally cost efficiency.

There are more and more tools proposing *continuous compliance* solutions. However, this may be discussed and decided prior to the development process as it could have an impact on the creative process of code writing. Furthermore, “continuous compliance is a relatively novel concept”. By definition, it means that a company maintains compliance with every code commit[25]. It is in this way a more proactive approach to code compliance.

In order to achieve continuous compliance, generally, an investment into third-party software is required. This software should integrate within the developer’s build system and/or repository so that as new code is committed, new Open Source dependencies can be evaluated. This allows to streamline issue management, reducing the time legal teams (and developers) are required to invest.”[26]

In Open Source, code audit is even more important as there are no barriers to third party inspection of the code. As the code is accessible, it can be reviewed by anyone making it easier to detect copyright infringement. This also expands the area of activity of patent-trolls, as they get more and more active in Europe.[27] Those “trolls” are persons or companies that depose patents without exploiting them. When they find uncompliant users of their protected Intellectual Property assets, they threaten them with legal suits.

The Open Source framework can as well be used for trolling activities, in a more indirect way. It is in this case not the patent, but the Open Source code released by someone who later searches for non-compliant users of his code in order to threaten them with legal suits.

---

[24] T.J. FOSTER & S.A. NORTHROP, *A Lawyer's Guide to Source Code Discovery,* February 2011. Available at : http://www.fedbar.org/Resources_1/Federal-Lawyer-Magazine/2011/February/Features/A-Lawyers-Guide-to-Source-Code-Discovery.aspx?FT=.pdf

[25] Pulsant, *What is Continuous Compliance, March 28, 2018.* https://www.pulsant.com/knowledge-hub/blog/what-is-continuous-compliance/

[26] T. UDELL, *A Case For Continuous Compliance*, May 16, 2019. Available at: https://fossa.com/blog/a-case-for-continuous-compliance/

[27] R. SCHESTOWITZ, *Patent Trolls Are Destroying Free/Open Source Software and They’re Coming to Europe, Thanks to the European Patent Office*, May 09, 2019. Available at: http://techrights.org/2019/09/05/patent-trolls-in-eu/

5.1.3 The operational phase of the audit

Usually, before operating the tool, non-disclosure agreements and a statement of work including estimations and details about the procedure of the review are signed.

First, a decision about the assignee of the code review has to be taken. In most cases, this operation is operated by specialized law firms in Intellectual Property and software issues. Those firms usually outsource the review and rather let a technical company process the actual review.

There are three different solutions about the place where the review can take place. It can take place in the premises of the requested law firms (which is the most frequent solution[28]), in a neutral environment or it can be done by using a remote control tool, which allows monitoring by the ordering party.

In terms of secured transfer of the code, choosing a law firm with expertise in the area of software audit guarantees a safer transfer procedure. As these firms often collaborate with technical reviewers, they normally have set up technical requirements (monitoring, limited access on the machines etc.) in order to prevent unauthorized copying of the code. It may as well be worthwhile to choose a reviewer whose premises are geographically not too far away from those of the developer in order to be able to assist the review in case of need and thus reducing costs.

Regarding the tool used by the reviewer, a discussion has to take place in identifying the need of complexity of this software. Regarding the disclosure of the code, the “NeedToKnow” concept may be the most secure way to go.[29] In this way, the source code is split avoiding the revelation of the entire code for one single person for example.

5.1.4 Conclusion

Source code audit is a very important task regarding business-sustainability in order to minimize risks of revenue losses or market opportunity. The most frequently, an audit of the code will be demanded if it comes to an acquisition of the product. As company acquisitions or merges can trigger very stressful situations, it is always helpful to have undertaken an audit in advance.

Being able to prove compliance in advance strengthens the position of force during negotiations. Furthermore, the conduct of a code audit is an investment in the future of a business as it is a great tool to avoid legal suits, to be aware of possible Intellectual Property rights infringement and to properly manage licensing of a product.

5.2 Source Code Audit Assessment Template

The aim of this template is to identify and assess the state and progress of legal source code audit of so far produced resources within the SPARTA project. Based on the legal source code audit guidelines, this template shall identify if recommended preparatory steps to source code audit as well as if practical code audit operations have been undertaken so far.

Project Acronym	Project Number

[28] Harbor Labs, *Guidelines for Source Code Review in Hi-Tech Litigation*, 2018.
Available at: https://harborlabs.com/assets/collateral/HL-WP10002-0618-CODE_REVIEW.pdf
[29] J. SAGASTUME, *Handing Your Software’s Source Code to Someone Else: When, Why and How?* June 7, 2019.
Available at: https://devops.com/handing-your-softwares-source-code-to-someone-else-when-why-and-how/

Each of the following issues should be addressed with a level of detail appropriate to the project.

The template has to be fulfilled for every produced software resource.

==========

RESOURCE *x:*

a. **Type of resource** (Description of the produced resource)

b. **Licensing and Copyright awareness training and provision of related documentation to developers** (Shall describe if and how developers of produced software code were trained on copyright and software licensing prior or during to the development of the code)

c. **Reverse code check-up procedure** (Shall describe the extend and recurrence of revers code check-up operations)

d. **Documentation procedure** (Shall describe the software documentation procedure of the produced resource)

e. **Summary of used third party licenses** (Shall describe, if any, the documentation of third party licenses, as forged Open Source code for example, used within the produced resource)

f. **Organization of the source code structure** (Shall describe the structuring of the source code directory, use of naming-schemes etc.)

g. **Audit procedure and method** (If audit operated, description of the procedure and method, internal or outsourced for example)

h. **Intellectual Property protection during audit operation** (Description of used Intellectual property protection tools for the audit operation, such as non-disclosure agreements for example)

Chapter 6 How to update the APER and the DMP?

The Assessment of Pre-Existing Resources (APER) and Data Management Plan (DMP) created by each of the research programs during the first six months of the project, were part of the effort to set up a proper governance system for the resources and in particular the data, needed to perform the initial research efforts.

It was already envisioned that there would be updates to these documents, as the research efforts would either necessitate to bring new “Pre-Existing Resources” into play, or they would at least generate new sets of data, that would have to be included in the existing DMP’s.

6.1 Updating the APER

As the research efforts progress, they may need the use of resources that were not initially identified but are pre-existing to the program. In such a case, an update of the APER is required.

The process itself is straightforward:

Step 1: A trigger is acknowledged. It will most likely be the addition of resources that were not initially foreseen to be part of the research effort but could have been as they were pre-existing.
Step 2: The program’s APER is updated with the new data and the corresponding assessments, as per the guidelines provided in Deliverable D.10.1.
Step 3: The updated APER document is sent to the WP10 Coordinator for review and consolidation of the global APER.

The analysis efforts conducted during the Step 2 of this process can be immediately re-used in the IDPR process described in Chapter 3 of this document.

6.2 Updating the DMP

The creation of new datasets will lead to updating the DMP. It is very likely that the research efforts will generate data and these will need to be assessed following the methodology proposed in D.10.2 – Data Management Plan. However, it could be possible that some of the research efforts or activities outcomes will not be data, and in such a case, updating the DMP wouldn’t be necessary.

We rely on the DMP process introduced in the Chapter 2 of the D.10.2 – Data Management Plan in order to propose a compatible process for the IDPR.

Step 1: A trigger for updating the DMP is acknowledged.
- 3 types of triggers can be identified: a request from WP10 to check for need to update, which would come before a project review. In such a situation, the minimal update of the document would be the fact that, in spite of data having been created, there would be no need for a modification of the DMP.
- A second trigger is simply the acknowledgement by the research team that new datasets have been generated during research work and need to be added to the DMP.
- The last trigger is a change in Consortium policies or composition, which may have an impact on the legal status of some assets (including data) and would require a new assessment of the datasets through an update of the individual DMP’s.

Step 2: The DMP owner conducts the necessary assessments and analysis.

Step 3: The updated DMP is sent to the WP10 Coordinator for review and consolidation of the global DMP.

The analysis efforts conducted during the Step 2 of this process can be immediately re-used in the IDPR process described in Chapter 3 of this document.

Chapter 7 Summary and Conclusion

Following the initial assessments conducted on assets used for research purposes, done through deliverables D.10.1 and D.10.2, the documentation of the present IDPR process led to highlight a few points. Before presenting them, it is useful to underline that the work already conducted on the APER and the DMP allowed to narrow the needs expressed in the process described in Chapter 3 of this document.

First, the breadth of issues that can be of interest is significant, and there is a serious risk of spending too much time and resources in analysing every legal aspect related to the research results. The best approach seems to focus first on the most sensitive and generic issues, i.e. legal challenges related to privacy and Intellectual Property, but also security of data and information. Other assessments may be postponed for times when the actual strategy for sustainable exploitation is known and efforts can be focused.

Next, the importance of formalising the process of identifying and documenting the produced resources has to be more documented. We do provide some insights, as a result of the preparatory work conducted for this deliverable. If the need for meta-data standards is clearly perceived in the research community, the privacy, intellectual Property and security assessments don't seem to be understood as immediate and generic requirements. For the sake of efficiency, there should be a more in-depth research work conducted on the different rationales, as it could help to provide also more specific requirements on which aspects of privacy obligations, intellectual Property needs and security requirements are the most generic and of significant importance.

Finally, it is important to highlight that the IDPR is supporting the increase in legal safety as it allows to keep the assessments, conducted through the generation of the DMP and the APER, up to date. This reinforces the sustainability of any further exploitation activity.

However, if there would be a topic offering room for improvement, we would consider the toolset related to the different levels of IDPR: beyond static documents, it could be interesting to develop a platform type of documentation sharing. The difficulty may lay in the maintenance efforts this would involve, which means the architecture of such a solution would have to be done so that it easily permits a sustainable deployment of such infrastructure. We suggest to use the work on deliverable D.10.5 in order to investigate this point a step further. It's very likely that this research, if applied, could lead to the design of an immediately available solution for other research works funded by the EU, or for the future EU Cybersecurity Competence Network and foster cybersecurity innovation in Europe.

Chapter 8 List of Abbreviations

Abbreviation	Translation
IDPR	Identification and Documentation of produced resources
DMP	Data Management Plan
APER	Assessment of pre-existing resources
OpenAIRE	Open Access Infrastructure for Research in Europe
CORDIS	Community Research and Development Information Service
EOSC	European Research Council
GDPR	General Data Protection Regulation
ENISA	European Network and Information Security Agency
ISMS	Information Security Management System
ISO	International Standards Organization
ECHR	European Court of Human Rights
TFEU	Treaty on the Functioning of the European Union
EU	European Union
IPA	Intellectual Property Analysis

Chapter 9 Bibliography

[1] CORDIS Webpage, https://cordis.europa.eu/about/en

[2] OpenAIRE Webpage, https://www.openaire.eu

[3] European Open Science Cloud (EOSC) strategic implementation plan, https://op.europa.eu/en/publication-detail/-/publication/78ae5276-ae8e-11e9-9d01-01aa75ed71a1/language-en

[4] Metadata Standards Directory Working Group, http://rd-alliance.github.io/metadata-directory/

[5] Organization for Economic Cooperation and Development (OECD), Recommendation of the Council concerning guidelines governing the Protection of Privacy and Transborder Flows of Personal data, 23th. September 1980

[6] European Court of Human Rights (Plenary), Klass and others v. Germany, 6th. of September 1978, application no. n. 5029/1971

[7] Regulation (eu) 2019/881 of the European parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[8] Regulation (EU) No 526/2013 (Cybersecurity Act) Article 5

[9] CASES; Monarc, https://www.monarc.lu/

[10] German Federal Office for Information Security: BSI Standards and Certification, https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

[11] European IPR Helpdesk, IPR management in software development, p.12, June 2013, https://iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-IPR-Management-in-Software-Development.pdf

[12] Opensource.com, What is Open Source, https://opensource.com/resources/what-open-source

[13] Dr. D. CROOKE, Open Source vs. Proprietary Software, https://www.greennet.org.uk/support/open-source-vs-proprietary-software

[14] M. DRIVER, Hype Cycle for Open-Source Software, July 11, 2016, https://www.gartner.com/en/documents/3371817/hype-cycle-for-open-source-software-2016

[15] M. WHEATLEY, Red Hat posts solid Q2 earnings, subscription revenue grows, September 21, 2016, https://siliconangle.com/2016/09/21/red-hat-posts-solid-q2-earnings-subscription-revenue-grows/

[16] M. DRIVER, Hype Cycle for Open-Source Software, July 11, 2016, https://www.gartner.com/en/documents/3371817/hype-cycle-for-open-source-software-2016

[18] Berne Convention for the Protection of Literary and Artistic Works, latest Text of July 24, 1971, Available at: https://global.oup.com/booksites/content/9780198259466/15550001

[19] Techopedia Dictionary: Software Licensing Definition, https://www.techopedia.com/definition/2558/software-licensing

[20] B. BYFIELD, Open Source Debate: Copyleft vs. Permissive Licenses, February 11, 2015, https://www.datamation.com/open-source/open-source-debate-copyleft-vs.-permissive-licenses.html

[21] Active State, License to Code: How to Mitigate Open Source License Risks, https://www.activestate.com/resources/white-papers/license-code-how-mitigate-open-source-license-risks/

[22] Open Logic, Open Source Software Audits: Why, When, and How to Conduct an Audit, April, 2011, https://www.roguewave.com/sites/rw/files/documents/white-papers/openlogic-open-source-audits.pdf

[23] Education Ecosystem Blog, 10 Tools for the Perfect Code Documentation, August 15, 2016, https://blog.education-ecosystem.com/code-documentation-tools/

[24] T.J. FOSTER & S.A. NORTHROP, A Lawyer's Guide to Source Code Discovery, February 2011, http://www.fedbar.org/Resources_1/Federal-Lawyer-Magazine/2011/February/Features/A-Lawyers-Guide-to-Source-Code-Discovery.aspx?FT=.pdf

[25] Pulsant, What is Continuous Compliance, March 28, 2018, https://www.pulsant.com/knowledge-hub/blog/what-is-continuous-compliance/

[26] T. UDELL, A Case For Continuous Compliance, May 16, 2019, https://fossa.com/blog/a-case-for-continuous-compliance/

[27] R. SCHESTOWITZ, Patent Trolls Are Destroying Free/Open Source Software and They're Coming to Europe, Thanks to the European Patent Office, May 09, 2019, http://techrights.org/2019/09/05/patent-trolls-in-eu/

[28] Harbor Labs, Guidelines for Source Code Review in Hi-Tech Litigation, 2018, https://harborlabs.com/assets/collateral/HL-WP10002-0618-CODE_REVIEW.pdf

[29] J. SAGASTUME, Handing Your Software's Source Code to Someone Else: When, Why and How?, June 7, 2019, https://devops.com/handing-your-softwares-source-code-to-someone-else-when-why-and-how/