D2.6

Initial Report on Legal and Ethical Aspects

WP2 – Guidelines and Procedures for System and Software Security and Legal Compliance

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/03/2022
Actual submission date: 31/03/2022

Responsible partner: POL
Editor: Luca Ardito
E-mail address: luca.ardito@polito.it

31/03/2022
Version 1.0

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The SIFIS-Home Project is supported by funding under the Horizon 2020 Framework Program of the European Commission SU-ICT-02-2020 GA 952652

Authors: Marco Ciurcina (POL), Giacomo Conti (POL), Maurizio Morisio (POL), Juan Carlos De Martin (POL)

Approved by: Joni Jämsä (CEN)

Revision History

Version	Date	Name	Partners	Section Affected Comments
0.1	20/12/2021	Defined ToC	POL	All
0.2	25/01/2022	UPGRADE 1	POL	All
0.3	08/02/2022	UPGRADE 2	POL	All
0.4	14/02/2022	First version	POL	All
0.5	20/02/2022	Second version	POL	All
0.6	21/02/2022	Updates	POL	All
0.7	23/02/2022	Updates	POL	All
0.8	25/02/2022	Ready for internal review	POL	All
0.9	27/03/2022	Revised after review	POL	All
1.0	31/03/2022	Ready for submission	POL	All

Executive Summary

This deliverable is the initial report on legal and ethical aspects regarding guidelines and tools to be developed in WP2.

It analyses 2 different topics:

1. management of legal obligations concerning the processing of personal data, particularly, obligations provided by Regulation (EU) 2016/679 (GDPR), providing techniques and tools that foster compliance by users of SIFIS-Home technologies and control by data subjects, including the management of communications among personal data controllers and data subjects;
2. management of legal obligations deriving from reuse and distribution of software according to the terms of free software / open source licenses or other free licenses.

The deliverable provides also an ethical analysis of the issues involved by the development and use of SIFIS-Home technologies by the different Agents involved (developers, users, data subjects, data processors and data controllers).

The final chapter provides a list of action points to be developed to include in SIFIS-Home technologies tools that foster compliance with GDPR and free software /open source licenses legal obligations.

Table of contents

1 Introduction

SIFIS-Home technology enters into a strict relation with people's private lives: it aims to provide technologies that work at home. However, applications connected to the internet can allow personal data to be communicated to third parties outside of home.

It is therefore very important to focus on legal and ethical analysis in order to design technologies that comply with privacy obligations provided by the GDPR and other applicable laws and fit the ethical goals of people using such technologies at their home: trust in SIFIS-Home technologies is crucial to foster its possible adoption.

Adoption of free/open source software is also useful to foster trust by users of the technology and the public at large; SIFIS-Home adopted this approach reusing and distributing free/open source software and applications. Therefore, it is also useful to provide tools that facilitate performing legal compliance analysis of the reused and distributed software.

2 Compliance with GDPR

Complying with GDPR is mandatory when processing personal data of *data subjects*, i.e. identified or identifiable natural persons.

When programming software that may be used to process personal data[1], software developers are not immediately obliged to follow GDPR's rules, as they may not be the ones that will personally process data. It is the act of processing[2] personal data that subjects them to GDPR's rules. Therefore, it is primarily who uses the software to process personal data or obtains personal data through its use, that has to be certain that his usage of software is compliant with the EU privacy rules.
Any information that relates to an identified or identifiable natural person is personal data[3]. This is a broad definition that includes everything that can be related, immediately or through some other information, to a specific individual and may be used to identify him, including by third parties.
Personal data can be **pseudonymised**, but this process is usually considered reversible. Therefore pseudonymised data remains personal data and falls within the scope of the GDPR.

Personal data can be **anonymised** in an irreversible way, so that the individual is no longer identifiable through the data collected. Truly anonymised data does not fall within the scope of the GDPR, as it is no longer considered personal data.

Annex 1 lists labels that identify the "Agents" involved with use of SIFIS-Home technologies as defined by GDPR and some "Actions" they can perform on data to protect personal data; Agents and Actions have definitions and legal source.

2.1 *Data controller, data processor and their obligations*

The **Data Controller**[4] is the subject (person or entity) responsible for the processing of personal data; it is the subject that determines the goals and the means of the processing. The Data Controller must be compliant with GDPR.
GDPR provides for a list of technical and organizational obligations to be complied with:

- effectively implement the principles set out in Article 5(1) GDPR
- meet the conditions of lawfulness set out in Article 6(1) GDPR
- comply with the constraints set out in Articles 9 and 10, GDPR
- provide information to the data subjects pursuant to Articles 13 and 14, GDPR
- respond to requests from data subjects and send notifications pursuant to Articles 15-22, GDPR

[1] According to article 4(1), point 1, GDPR "*'personal data' means any information that relates to and 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*".

[2] According to article 4(1), point 2, GDPR "*'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

[3] As per article 2 GDPR. A non-exhaustive list of examples could include a home address, the name or surname of somebody, his IP address, photos of him, video recorded inside his house and so on.

[4] According to article 4(1), point 7, GDPR, "*'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".

- protect data by design and by default pursuant to Art. 25, GDPR
- make agreements with joint controllers and/or contracts or other legal acts with processors pursuant to Articles 26 and 28, GDPR
- drafting instructions to persons acting under the authority of the controller or of the processor and training them pursuant to Article 29, GDPR
- keeping the register of processing activities pursuant to Article 30, GDPR
- ensuring a level of security appropriate to the risk pursuant to Article 32, GDPR
- notifying the Privacy Supervisory Authority and notifying the data subject pursuant to Articles 33 and 34, GDPR
- carry out the data protection impact assessment pursuant to Article 35, GDPR
- carry out the prior consultation pursuant to Article 36, GDPR
- designate the data protection officer pursuant to Article 37, GDPR
- adhere to codes of conduct and/or adopt certifications pursuant to Articles 40-43, GDPR
- comply with the conditions for the lawfulness of data transfer abroad pursuant to Articles 44-50, GDPR
- provide information about cookies pursuant to national laws implementing Article 5(3) of the ePrivacy Directive 2002/58/EC, as amended by 2009/136/EC.

Among those obligations, it doesn’t seem possible to facilitate the compliance of the organizational ones through SIFIS-Home technologies. However, compliance with the following obligations could, instead, be fostered by SIFIS-Home technology:

- effectively implement the principles set out in Article 5(1) GDPR
- provide information to the data subjects pursuant to Articles 13 and 14, GDPR
- receive consents provided by Articles 6(1), 9 and 49(1) GDPR
- respond to requests from data subjects and send notifications pursuant to Articles 15-22, GDPR
- protect data by design and by default pursuant to Art. 25, GDPR
- make agreements with joint controllers and/or contracts or other legal acts with processors pursuant to Articles 26 and 28, GDPR
- ensuring a level of security appropriate to the risk pursuant to Article 32, GDPR
- notifying the data subject pursuant to Articles 34, GDPR
- carry out the data protection impact assessment pursuant to Article 35, GDPR
- comply with the conditions for the lawfulness of data transfer abroad pursuant to Articles 44-50, GDPR
- provide information about cookies pursuant to national laws implementing Article 5(3) of the ePrivacy Directive 2002/58/EC, as amended by 2009/136/EC.

Whoever determines the purposes and means of the processing of personal data automatically becomes a Data Controller. The identified or identifiable natural person to whom personal data relates is, instead, the Data Subject[5]. There can be several Data Controllers, who "*determine the purposes and means of the processing of personal data*"[6]. In this case, they're called Joint Controllers.
The Data Controller will be the subject responsible for the correct processing of personal data.
There are different obligations that the GDPR imposes to the Data Controller.

On a general level, the Data Controller must adhere to a list of **principles**[7]. "*Personal data shall be:(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');*
*(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**');*
*(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');*
*(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');*
*(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation**');*
*(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').*
*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**')*".

The Data Controller must ensure that the individual whose data is processed (the Data Subject) is correctly informed of the processing and of his rights. To do so, the Data Controller can create a Privacy Notice: a document that is then communicated to the Data Subject. This is made explicit in articles 13 and 14[8], which mandate for "*sufficient information*" that must be given to the subject. Article 13 regards data obtained directly from the data subject, while article 14 is about data obtained from third parties, but in both cases the aim is the creation of a proper Privacy Notice, able to correctly inform the Data Subject in a clear and plain language. A more detailed analysis of the content of Privacy Notice is performed in chapter 2.5.
There are other GDPR obligations that provide for exchange of communications among Data Controllers and Data Subjects and among Data Controllers and Data Processors and therefore could be relevant for SIFIS-Home technologies:

- receive consents provided by Articles 6(1), 9 and 49(1) GDPR
- respond to requests from Data Subjects and send notifications pursuant to Articles 15-22, GDPR

[5] Article 4 (1), GDPR
[6] Art. 4 (6), GDPR
[7] See article 5, GDPR
[8] A list of information to be provided can be found in chapter 2.5 of this document, "Privacy Notice"

- make agreements with Joint Controllers and/or contracts or other legal acts with Data Processors pursuant to Articles 26 and 28, GDPR
- notifying the Data Subject pursuant to Articles 34, GDPR
- provide information about cookies pursuant to national laws implementing Article 5(3) of the ePrivacy Directive 2002/58/EC, as amended by 2009/136/EC.

Articles 25(1)[9] obliges the Data Controller to put into place appropriate technical and organisational measures to protect the rights of Data Subjects "by design". Article 25(2)[10] oblige the Data Controller to implement appropriate technical and organisational measures for ensuring privacy "by default".
Article 32[11] provides for obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
Then, article 35 mandates him in some cases to carry out a Data Protection Impact Assessment. This will be analysed in more details later in chapter 2.6.

The concept of Data Controller is strictly bound to that of **Data Processor**: "*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*"[12]. The Data Processor must comply with security obligations provided by article 32, GDPR, and must adhere to the instructions provided by the Data Controller according to the contract or other legal act concluded among them according to article 28(3), GDPR: if the Data Processor acts without the Data Controller's instructions in such a way that it determines the purpose and means of processing it will be considered as a Controller in respect of that processing and will have the same liability as a Data Controller[13].

[9] According to article 25(1), GDPR, "*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*".

[10] According to article 25(2), GDPR, "*The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*".

[11] According to article 32(1), GDPR, "*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
(a) the pseudonymisation 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 organisational measures for ensuring the security of the processing.".
According to article 32(1), GDPR, "*In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*".

[12] Article 4 (8), GDPR.

[13] As provided by article 28(10), GDPR; see also ICO: Information Commissioner's Office, *What are "controllers" and "processors"?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#:~:text=a%20processor%20as%3A-,'processor'%20means%20a%20natural%20or%20legal%20person%2C%20public%20authority,interests%20rather%20than%20their%20own.

If the processing happens in a cloud-based system and personal data is materially stored in third-party servers, and the cloud client determines the means and the purposes of the processing, he is the Data Controller and the Cloud provider, on the other hand, is considered as a Data Processor.

2.2 *The Software Developer*

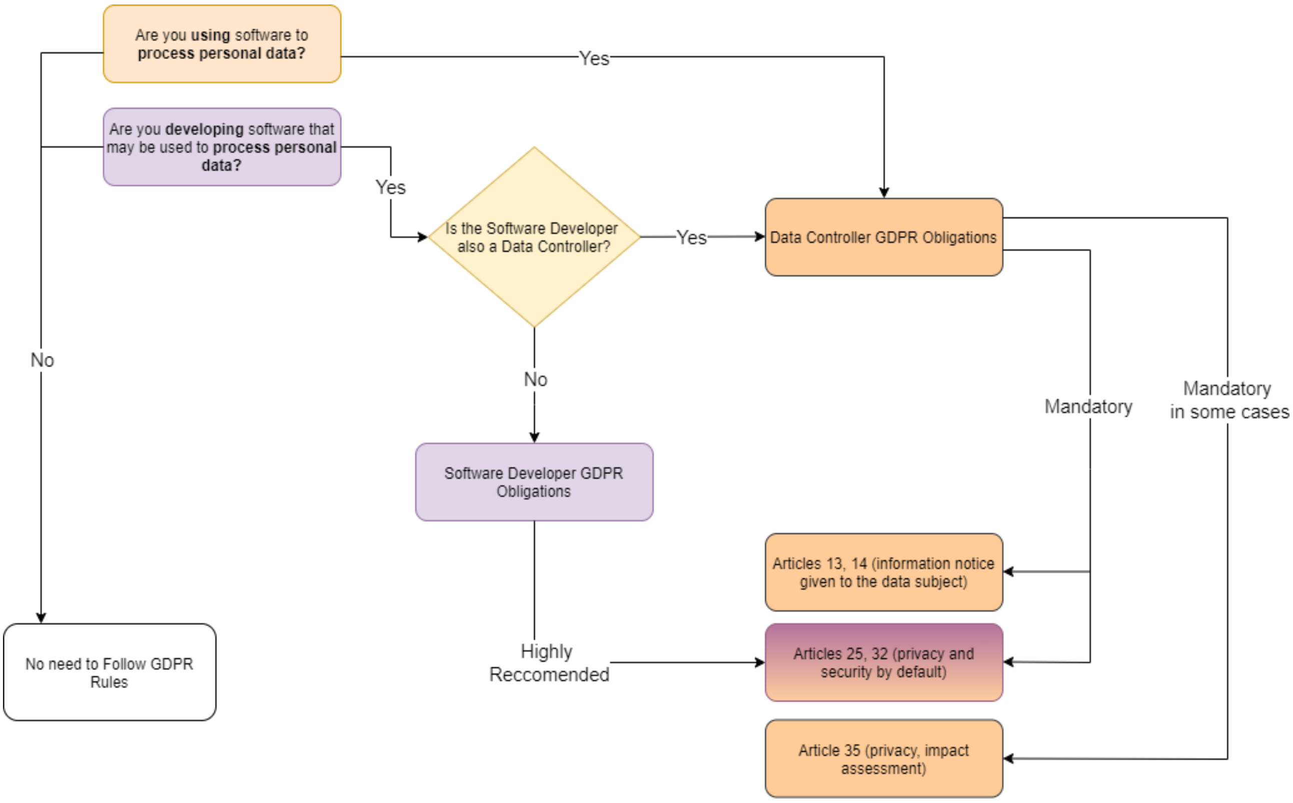
This consideration brings us to another third party subject, the **Software Developer,** who develops a software which may be used to process personal data by the same software developer (for example, when a registration has to be completed for the software to be usable), or by third parties (such as when a software is used to record video from a location through a camera).

The software developer **may or may not be Data Controller himself.** He/she becomes Data Controller when they themselves use such a software to process personal data. But, regardless of he/she is or not a Data Controller, he/she has interests in following GDPR articles 25 and 32, and to provide the end user with a software that easily allows for privacy-compliance. If the developed software is used to process personal data by the end user, in fact, then it will be this end user that will become the Data Controller.

Before, we saw how Article 25 introduced the concepts of *data protection by design* and *data protection by default.* Article 32, on the other hand, was about the concept of *security of processing.*

Data protection by design and by default can be obtained through:
1) Up-to-date techniques to process personal data and to store it securely, taking into account the state of the art and the cost of implementation.
2) Appropriate technical and organizational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are being processed.

Despite the fact that the Software Developer is not obliged to keep in mind these GDPR rules while programming, as he/she may not be the Data Controller, it is recommended that he/she does so if the software has to process personal data. This is because if the software is used for personal data processing, then someone, somewhere, will sooner or later inevitably become Data Controller and will therefore have to be compliant with GDPR obligations, such as the aforementioned 13, 14, 25**,** 32 and 35.


Are you using software to process personal data?
Are you developing software that may be used to process personal data?
Yes
Yes
Is the Software Developer also a Data Controller?
Yes
Data Controller GDPR Obligations
No
No
Software Developer GDPR Obligations
Mandatory
Mandatory in some cases
Articles 13, 14 (information notice given to the data subject)
No need to Follow GDPR Rules
Highly Reccomended
Articles 25, 32 (privacy and security by default)
Article 35 (privacy, impact assessment)

A summary of the obligations GDPR imposes on the Data Controller and, potentially, on the Software Developer.

Getting a software to be GDPR-compliant is no easy task and it cannot be done exclusively by the software designer, nor it can be done completely through the use of automated tools (at least for now). Every Data Controller must be sure that their specific way of processing personal data is compliant with the current legislation, but it can be argued that a privacy-conscious software may very much help them to reach this objective.
There are already some automated tools that can aid a Data Controller to be GDPR-compliant, such as ICO's Lawful Basis Interactive Guidance tool[14], although they all require a self-assessment from the user and are at the moment not able to automatically determine whether a processing is compliant or not. In this sense, a sort of a dashboard can be helpful in more easily evaluating whether the personal data processing method is GDPR compliant or not.

2.3 *Organisational Obligations*

Compliance to the GDPR requires "*appropriate technical and organizational measures*", something which is only partly obtained through what's been shown in the previous chapter.
Technical and organisational measures are the processes, control systems, procedures and measures taken to protect and secure the personal information that an organisation processes.

Recital 78, GDPR, exemplifies what these measures are concretely, although giving a non-exhaustive list: "*such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features*[15]".

[14] Available at https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/
[15] Recital 78, GDPR

It is the **Data Controller** that has the obligation to make sure that there are sufficient organizational and technical measures in place. These attain to risk analysis, organisational policies, and physical and technical measures, which are impossible to define once and for all in the legislative text, but are varied, and based upon the scope of the processing, the state of the art and the cost of implementation.

This means that no two Data Controllers will follow the same exact organizational and technical measures. A small dentists' studio will not be required to have measures to keep their patients' data safe and secure like a huge public hospital, as the magnitude of the processing, the economic possibilities and the risks involved are very different between the two. Also, it is important to notice that even if standard organizational and technical measures are put in place, other measures may be needed depending on the circumstances and the type of personal data processed. The requirement, therefore, is flexible.

What follows here is a list of steps to undertake in order to be compliant with this GDPR's request[16].

- Perform a risk assessment: understand the appropriate level of security the data controller needs to put in place.
- When deciding what measures to implement, take account of the state of the art and costs of implementation.

- If needed, create an internal information security policy (or equivalent) and take steps to make sure the policy is implemented.
- Whenever a policy is set, ensure that there are controls in place to enforce it.
- Regularly review the information security policies and measures and, where necessary, improve them.
- Use encryption and/or pseudonymisation where it is appropriate to do so.
- Make sure that it is possible to restore access to personal data in the event of any incidents, for example by establishing an appropriate backup process.
- Conduct regular testing and reviews of the measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. Also keep an eye out for technological progress, as what is one year's state-of-the-art may not be the next year's.
- Where appropriate, implement measures that adhere to an approved code of conduct or certification mechanism.
- Ensure that any data processor, which processes personal data on behalf of the controller, also implements appropriate technical and organizational measures.

2.4 *Data Controllers in smart-home environment*

In a smart-home environment, four main Agents can be identified. They are (i) the software developer; (ii) the home owner who uses these types of software in his house; (iii) the people who, upon entering the house, have their personal data processed through smart-home applications; and (iv) the cloud service provider, whose service is storing personal data coming from the user's house.

[16] These are suggestions coming from the ICO, UK's authority on privacy and GDPR compliance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

While it is undoubtedly true that smart-home software can process personal data, it can appear unreasonable that home owners who install smart home devices inside their property are always forced to become Data Controllers and be burdened with all the obligations that the GDPR entails.

This is a long-standing problem. The European Directive that is the antecedent to the GDPR, Directive 95/46, stated that it should not apply to the processing of personal data done by a natural person in the course of a purely personal or household activity[17]. This is called the "household exception". As the same exact wording is used in Article 2 (2) (c) of GDPR, it can be inferred that in this case the same doctrine which was born from Directive 95/46 can apply to GDPR.

The first consideration that has to be done is defining where and when such an exception can take place. The European Court of Justice ruled in 2014 that *only activities that take place on a private area can be considered "personal"*"[18]. The Court also stated that only activities "*which are carried out in the course of private or family life of individuals*" are relevant for the household exception, and this is not the case if the processing of personal data consists "*in publication on the internet so that those data are made accessible to an indefinite number of people*"[19].

Therefore, "*the user of video surveillance at home needs to look at whether he has some kind of personal relationship with the data subject, the scale or frequency of the surveillance suggests some kind of professional activity on his side, the surveillance's potential adverse impact on the data subjects.*

The presence of any single one of the aforementioned elements does not necessarily suggest that the processing is outside the scope of the household exemption, an overall assessment is needed for that determination" (EDPB, 2019).

In the last years, the European Court of Justice gave relevance to the concept of Joint Controllers[20]: multiple entities who share responsibility for the correct processing of personal data. Starting from 2014, the Court widened the joint controllership concept[21].

For smart-home application designers, "*the widening scope of joint controllership means that they may well fall within the definition of a joint controller, as they are the ones defining in technical terms how smart home data are collected and for what potential purposes*" (Chen, 2020).

This concept has to be mediated with the household exception. But, even if the exception applies, it can only be related to the home owner, and not to the software developer. This is because developers are often not just individuals, but are part of a larger structure, such as a software company. Moreover, in many cases they are doing their work *professionally with commercial intent*. These characteristics, if present, exclude them from the household exception.

GDPR's recital 78 explains that "*when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.*". This seems to indicate that software developers are not

[17] Article 3(2), Directive 95/46/EC, *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN , 24 October 1995

[18] Case C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62013CJ0212&from=EN, 11 December 2014

[19] Case C-212/13, ibid.

[20] As per article 26 GDPR: "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation. […]"

[21] Such as in the famous *Google Spain* court case, also named *Costeja*, in which the responsibility of the search engines for the treatment of the personal data that happens when pages of third parts, indexed on the same engine, contain personal data of individuals (in the so-called snippet), was determined.

immediately categorized as Data Controllers (Chen, 2020). In smart homes, they do not determine the overall purpose of the system, but only offer technical solutions. The key word here is “encouraged”. They are not obliged to take into account the rights of the data subjects, but it is strongly recommended for them to do so while programming their software.

There are no clear-cut answers to the role of software developers and smart-home owners. But even if both the owner and other Agents are indeed Joint Controllers, the Court has stated that “*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*”[22].

It is clear that current data protection law does not offer a complete, explicit and throughout regulation of what happens inside smart homes, nor does it offer a comprehensive methodology to assess the roles and responsibilities of each subject involved.

Smart-home software development should therefore take into account these issues.

Then, it should also offer state of the art ways to process personal data in a secure and privacy conscious way, and ensure that Data Controllers (including home owners that choose to process personal data as Data Controllers) can comply with GDPR and the Data Subjects are able to effectively exercise their rights to data protection. It should also tell the end user (the home owner and possibly Data Controller) what kind of data gets processed and, if a cloud service is used, where that data eventually ends up.

It will be up to the user to ensure that the personal data processed by their smart-home devices complies with GDPR, if it applies. Because the boundaries of the household exception are not clear cut, it’s a reasonable option to provide for the possibility that the home owner makes his decision about complying with GDPR or not.

2.5 *The Privacy Notice*

An important requirement when processing personal data is to submit a Privacy Notice (PN) to the Data Subject. The Privacy Notice is a document that must be drafted by the Data Controller and explains how and why personal data is processed; for how long and in which way the Data Subjects can exercise their rights. It is important that the PN is written in an easy to understand manner, and must be presented to the Data Subjects when their data gets processed[23].It is possible to divide the Privacy Notices’ requirements into two: stylistic requirements and content requirements.

Regarding the stylistic requirements, the PN must be:

- Written in a concise, transparent, intelligible, and easily accessible form.
- Written in clear and plain language, particularly for any information addressed specifically to a child.
- Delivered in a timely manner, before the processing happens.
- Provided free of charge.

Regarding the content requirements, the PN must include the following information:

- The identity and contact details of the organization, its Data Controller and its Data Protection Officer, when present.

[22] See the *Wirtschaftsakademie* court case, https://curia.europa.eu/juris/document/document.jsf?text=&docid=204508&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1367796

[23] Articles 12 and 13 GDPR

- The purpose of the processing: why is that data needed, and what is the legal basis for the processing and, if applicable, the legitimate interests pursued by the Data Controller or by third parties?
- The recipients or categories of recipients of the personal data, if any.
- The details regarding any transfer of personal data to a third country, if that could happen, and the safeguards taken.
- A specification of the period during which the data collected is retained. This time period must be specifically limited and cannot be forever.
- The existence of each data subject's rights: access, rectification, portability, erasure. Also, the right to revoke consent at any time[24].The right to lodge a complaint with a supervisory authority.
- The existence of an automated decision-making system, including profiling, and information about how this system has been set up. In any case, this automated decision-making system cannot by itself produce effects on the Data Subject, but it needs a human being to eventually confirm its decisions.

Moreover, if personal data is acquired from the Data Subject, the Data Controller must provide information about whether the provision of personal data is a legal or contractual obligation or a necessary requirement for the conclusion of a contract, and whether the Data Subject is under an obligation to provide personal data, as well as the possible consequences of failure to provide such data.

Instead, if personal data is not acquired from the Data Subject, the Data Controller must provide information about the categories of personal data concerned and the source from which the personal data originate and, where applicable, whether the data come from publicly accessible sources.

If cookies are used, then the Data Subject must be informed about their presence, whether they are necessary to provide services or not, and if not how to avoid them (for example by setting up their browser in such a way as to automatically refuse them), the purposes of the cookies and the period of their storage.

The GDPR.eu webpage offers some suggestions on how to build an effective Privacy Notice by simply formulating precise and complete answers to certain questions[25], therefore dividing the PN into as many paragraphs as these same questions:

- What data is collected?
- How does this organization collect personal data?
- For what purpose will that data be used?

[24] Right of access: the Data Subjects must be able to access their data as soon as possible after submitting a request.
Right of rectification: the Data Subjects must be able to ask for their data to be modified.
Right of portability: the Data Subjects must be able to make copies of their processed data.
Right of erasure: the Data Subjects must be able to revoke their consent at any time and to force the erasure of their data from the organization's database.

[25] See https://gdpr.eu/privacy-notice/

- How will that data be stored?
- Are there third parties who will receive that data? If so, who are they, and why do they receive it?
- What are the data protection rights offered to the user? (access, rectification, portability, erasure).
- What are cookies?
- How are cookies used in this webpage/service?
- What types of cookies are used?
- How to manage cookies?
- How and when do changes to this privacy policy occur?[26]
- How to contact the organization?
- How to contact the appropriate authorities?
- Is an automated decision-making system, including profiling been implemented? If yes, how this system has been set up?
- If personal data is acquired from the Data Subject, is the provision of personal data a legal or contractual obligation or a necessary requirement for the conclusion of a contract? Is the Data Subject is under an obligation to provide personal data? What are the possible consequences of failure to provide such data?
- If personal data is not acquired from the Data Subject, what categories of personal data are processed? From which source the personal data originate? Does the data come from publicly accessible sources?

Some tools may help both the Data Controllers to build PNs compatible with GDPR[27]. This could be a dashboard to be manually filled out by the Data Controller, who will self-assess his privacy notice and check if it respects all the requirements that the GDPR imposes. The idea here is to present these requirements one after the other to the Data Controller, so that he/she can reflect on how he approached those during the writing of the privacy notice without forgetting any of them. Some information (as way of example, the categories of personal data processed) could be automatically proposed to the Data Controller by the tool. A solution like this is also important for the Data Subject. Generally speaking, is important that the Data Subject understands and pays attention to the privacy notice provided by the Data Controller, and that the Data Controller provides a complete privacy notice, compliant to the European rules. By using a dashboard or a similar tool, the Data Subjects get an easy to read screen where they can quickly understand how their personal data is processed, and if that processing is respectful of the rules and generally fine for them. Moreover, some information could be prefilled automatically depending on the characteristics of the technology adopted.

[26] Data controllers are invited to keep their privacy policy under regular review and make it so that any updates to it can be easily.

[27] Such as CNIL's open source PIA software, highlighted later in this chapter and also in chapter 3

2.6 *The Privacy Impact Assessment*

The Data Controller should sometimes assess which privacy risks the software may pose to users and Data Subjects alike[28]. This happens when the processing could result "*in a high risk to the rights and freedoms of natural persons*", and is particularly relevant when new tools or a new technology are used to process personal data (ARTICLE 29 WP, 2017).
Concerning the definition of "high risk", Article 35 (3) offers some examples of "high-risk processing":

1) When the processing results in a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly affect the natural person in a significant way;
2) When the processing is related to a large number of special categories of data[29];
3) When large-scale, systematic monitoring of a publicly accessible area is conducted.

For "special categories of data" the GDPR means those information that are especially sensitive and regard peculiar traits or conditions of the individual, such as its ethnic origin or religious and political beliefs[30], or relating to criminal convictions and offences[31]. This kind of data should not be processed, except for peculiar reasons shown in article 9, the main of which is the explicit consent of the Data Subject to the processing of those personal data[32].
In any case, the Privacy Impact Assessment (PIA), when required, must be carried out prior to the processing. If the subject carrying out this processing is an organization with a Data Protection Officer[33], then this person must be consulted before proceeding with the processing.
The PIA itself must contain four key elements:

1) A systematic description of the intended processing operations and the purposes of the processing, including the legitimate interests pursued by the Data Controller;
2) An assessment on the necessity and proportionality of the processing operations in relation to the purposes;
3) An assessment of the risks to the rights and freedoms of Data Subjects;
4) The measures put in place to mitigate the risks and to ensure the protection of personal data.[34]

This means that conducting a PIA requires the assistance of personnel who are highly skilled not only in data protection but also in systems security.
Although there can be other subjects involved in the creation of a Privacy Impact Assessment, such as the DPO, the legal responsibility lies always on the Data Controller.

[28] CNIL, *Privacy Impact Assessment Methodology*, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf
[29] Categories which are explicated in articles 9 and 10 GDPR.
[30] The complete list given by article 9 is this: "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".
[31] Article 10 GDPR.
[32] More information on the requirements of a Privacy Impact Assessment, and the cases where it's needed, can be found in WP 2.2.
[33] The Data Protection Officer is a role whose aim is to independently ensure that an organization is compliant with the laws protecting personal data.
[34] GDPR.eu, *Data Protection Impact Assessment (DPIA)*, https://gdpr.eu/data-protection-impact-assessment-template/

As it was previously shown in Deliverable 2.2 "Preliminary Developer guidelines", there are some external tools that can support Data Controllers in building and demonstrating compliance to the GDPR. The French CNIL[35] created a useful tool[36] that has quickly become the reference standard. Using this tool can help the developer to understand the security and privacy risks posed by his software and may give him the chance to solve them before shipping his product to the public. Another interesting, albeit less interactive "tool" is the PIA template provided by the ICO through GDPR.eu[37].

Again, just like it was in regards to GDPR compliance as a whole, it is not the Software Developer who is responsible for preparing a PIA per se.

However, the fact that he/she is creating a software which may be used for types of processing requiring a Privacy Impact Assessment makes this a matter of opportunity. Whoever uses this kind of software to process specific kinds of personal data, or personal data in a specific way, be it the software developers themselves or a separate final user, becomes a Data Controller and could therefore be obliged to perform a Privacy Impact Assessment.

It is therefore highly recommendable for the software developer to make available as much information useful to perform a PIA as possible, therefore aiding the subsequent Data Controller in complying with art.35 of GDPR.

3 Techniques and tools for processing personal data

In the previous chapter, numerous requirements have been identified that need to be taken into account to create software which is GPDR-compliant, and to be GDPR-compliant when using that same software in order to process personal data.

Here, a list of common techniques and tools to aid both software developers and general Data Controllers in managing which information has to be given to the Data Subjects is presented. These tools are useful both to create a Privacy Notice or check the compliance of an existing one, and to complete a Privacy Impact Assessment. It must be stressed however that compliance in general cannot be truly checked in an automated way: GDPR is centered around principles and allows competing interests to be balanced against each other. It does not mandate specific actions. Thus, certain kinds of processing are neither clearly legal or illegal – it depends on the context.

EDPS' Website Evidence Collector – https://edps.europa.eu/edps-inspection-software_en. This is an open source software tools for the automation of privacy and personal data protection inspections of websites. The collected evidence, structured in a human- and machine-readable format (YAML and HTML), allows website controllers, data protection officers and end users to understand better which information is transferred and stored during a visit of a website.

CNIL's open source PIA software - https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
Already seen in the previous chapter, this software aims to help data controllers build and demonstrate compliance to the GDPR. It facilitates carrying out a privacy impact assessment.

ICO's PIA template - https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf
Seen in the last chapter, this template allows the data controller to quickly gauge the main requirements of a privacy impact assessment

[35] CNIL is France's independent administrative regulatory body to ensure that data privacy law is enforced in the French territories.

[36] Downloadable on the official CNIL's website: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

[37] Which can be found at https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

Reddit's Privacy Policy - https://www.redditinc.com/policies/privacy-policy-september-12-2021 The famous internet website and forum reddit provides a well-made privacy policy, divided into specific subjects, easy to read and to understand and well-presented graphically. It can be used as a source of inspiration for more privacy policies.

4 License obligations

Development of software reusing software available under a free software / open source license and distribution under the same licenses by the SIFIS-Home project implies the need to comply with the legal obligations provided by such licenses.

Artifacts that are not software (like datasets, texts, images and pictures) that adopt free licenses (that is, licenses with the same characteristics of free software /open source licenses but that are designed to work for other artifacts[38]) could also be reused and distributed by the SIFIS-Home project.

4.1 *Free software / open source licenses characteristics*

The most relevant aspect of free software / open source licenses is whether or not they include a copyleft clause. A copyleft clause is a clause of the license that provides for the right of the user to modify and redistribute the software licensed under the license provided that the modified version is in turn licensed under the terms of the same license.

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

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

First, there are non-copyleft licenses, i.e. licenses (such as the BSD[39], MIT[40] and Apache[41] licenses) that do not contain a copyleft clause and therefore have no copyleft effect: who distributes a software available under a non-copyleft license is not required to distribute it under the terms of the same license.

Then, there are the so-called strong copyleft licenses: these are licenses that contain copyleft clauses extending their effects to all derivative works, including software libraries that, when executing a software licensed under a strong copyleft license, are linked dynamically to it[42].

The licenses that, however, narrowly restrict the scope of the copyleft clause, thus allowing different licenses to be applied to some derivative works, are called weak copyleft licenses; among them the GNU Lesser General Public License (GNU-LGPL)[43] and the Mozilla Public License (MPL)[44].

There are also some licenses, such as the GNU General Public License (GNU-AGPL)[45] and the European Union Public License (EUPL)[46], which require that the source code of the program is available also to users who use the software remotely, connecting to the server at which the software is run as a service (called SaaS): these licenses are called network copyleft.

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

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

[38] Definitions that apply to other artifacts and have content substantially similar to the definition of free software / open source are the definition of free cultural work (see https://freedomdefined.org/Definition) and the open definition (see http://opendefinition.org/od/2.1/en/).

[39] For the last version see https://www.freebsd.org/copyright/freebsd-license.html).

[40] See https://mit-license.org/.

[41] For the last version 2.0 see https://www.apache.org/licenses/LICENSE-2.0.

[42] The extension of the copyleft effect of the strong copyleft licenses is debated and depends on legal details of different legal systems; on this see http://www.ifosslr.org/public/LinkingDocument.odt cited in Bain, 2010).

[43] For the last version 3.0 see https://www.gnu.org/licenses/lgpl-3.0.en.html.

[44] For the last version 2.0 see https://www.mozilla.org/en-US/MPL/.

[45] For the last version 3.0 see https://www.gnu.org/licenses/agpl-3.0.html.

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

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

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

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

4.2 *Reuse and distribution*

Free software licences impose a series of obligations on those who distribute the software in its original or modified version.

Therefore, anyone who distributes (on physical media or even online) copies or modifications (so-called patches) of free software or who distributes products that include free software components must comply with these obligations.

In some cases, even the offer of software as a service (so-called SaaS) may imply the need to comply with some obligations imposed by free software licenses (for instance, if you use network copyleft software on the server 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 on who distributes the artifact. Nonetheless, those obligations, while typical of this type of licenses, 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 (e.g., GPL and MPL),
- to hold harmless the software contributors from any damages resulting from the distribution of products that include the software itself (e.g., the EPL).

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 (e.g., MIT and Apache licenses),
- to give credit to the authors of the artifact (e.g., original MITv1 and BSD licenses),
- for the case you change the artifact, to indicate which changes have been introduced (e.g., 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, cause 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 or other systems to fetch all source code of the projects and their dependencies,
- 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.

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 are incompatible with each other. Then, reusing artifacts licensed with different free licenses, it is crucial to analyse how the different components interact to avoid the risk of incompatibility.

5 Information, procedures and tools for free software / open source licenses compliance

Information, procedures and tools that ease compliance with legal obligations provided by free software / open source licenses are well documented and widespread.

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[47];
- the Open Source Initiative website that lists licenses that comply with the Open Source Definition and provides other information[48];
- the Wikipedia webpage that provides information about most of the free software licenses (e.g., https://en.wikipedia.org/wiki/Apache_License) including comparison of free and open-source software licenses[49];
- the Choose a License website[50], the tldrLegal website[51] and the Joinup Licensing Assistant (JLA) website[52] that provide information about some of the most well-known free licenses and the obligations to be complied with according to each of them.

The “Open Compliance Program” of the Linux Foundation[53] provides information and tools the support in organizing a compliance procedure.

[47] See https://www.gnu.org/licenses/.

[48] See https://opensource.org/licenses.

[49] See https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses.

[50] See https://choosealicense.com/.

[51] See https://tldrlegal.com/.

[52] See https://joinup.ec.europa.eu/collection/eupl/joinup-licensing-assistant-jla.

[53] See https://compliance.linuxfoundation.org/.

The Linux Foundations supports the SPDX standard[54] 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[55], that provides the OpenChain ISO/IEC 5230, an International Standard for open source license compliance consisting of a set of requirements for compliance programs, materials and tools useful to set a compliance program and perform compliance tasks.

In the frame of the OpenChain project it was recently presented the OSS Review Toolkit (ORT)[56], that makes available a customizable pipeline of tools useful in the frame of a legal compliance analysis.

Many projects are working on the development of useful tools that help in performing legal compliance tasks.

FOSSology[57] is a free software license compliance software system and toolkit that allows to run license and copyright scans.

ScanCode toolkit allows to detect licenses, copyrights, etc. in software reused[58].

Reuse Software project[59] provides a set of recommendations to make easier to choose and provide licenses, add copyright and licensing information to each file and confirm compliance and provides a tool to automate some of these steps.

The Open Source Initiative launched the ClearlyDefined[60] project, that aims to support projects in clearly describing their projects, the licenses adopted and security vulnerabilities[61].

Other useful tools are:

- Ninka, a license identification tool[62];
- Open Source License Checker, a license identification tool[63];
- Tern, a tool that generates a software Bill of Materials for container images and Dockerfiles[64];
- Hermine[65] is a tool to manage bill of materials of software components, their licenses and their respective obligations.

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[66] and provides information about license attribution[67].

For datasets, it is worth mentioning the licensing assistant made available by the European Data Portal[68].

6 Ethical analysis

An outline analysis of the ethical profiles involved by the development and use of SIFIS-Home technologies is provided below.

[54] See https://spdx.dev/ids/.

[55] See https://www.openchainproject.org/.

[56] See https://github.com/oss-review-toolkit/ort.

[57] See https://www.fossology.org/.

[58] See https://github.com/nexB/scancode-toolkit.

[59] See https://reuse.software/.

[60] ClearlyDefined was also proposed in D2.2 as one of the possible solutions to obtain a “green light” regarding privacy and security compliance.

[61] See https://clearlydefined.io/about.

[62] See http://ninka.turingmachine.org/.

[63] See https://sourceforge.net/projects/oslc/.

[64] See https://github.com/tern-tools/tern.

[65] See https://gitlab.com/hermine-project/hermine.

[66] See https://creativecommons.org/choose/.

[67] See https://wiki.creativecommons.org/wiki/Best_practices_for_attribution.

[68] See https://www.europeandataportal.eu/en/content/show-license.

The Agents[69] involved in the development and use of SIFIS-Home technologies can be classified into different categories:

- Agents that develop SIFIS-Home technologies;
- natural persons that use SIFIS-Home technologies in the course of a purely personal or household activity;
- natural persons that use SIFIS-Home technologies as data subjects;
- Agents that use SIFIS-Home technologies as data processors; and
- Agents that use SIFIS-Home technologies as data controllers (including SaaS providers).

The ethical analysis of SIFIS-Home technologies is carried out starting from the fact that, in addition to enabling various features for the Agents that use it (controlling the operation of devices to turn the light on and off, the oven, etc.), they enable relations between different Agents that can imply the processing of personal data.

6.1 *The ethical values*

The ethical options for the different Agents are analysed in the light of the goal of protecting value and dignity of all human beings.

In order to do so, protection of fundamental rights of natural persons is given a higher value over protection of interests of different Agents (legal person, including companies, public authority, agency or other body).

Therefore, the analysis is carried out by making a simplifying assumption: all Agents are natural persons and the golden rule[70] "*do not treat others in ways that you would not like to be treated*" is applied.

According to the above, a list of ethical issues involved in the development and use of SIFIS-Home technologies follows. It is worth to highlight that this choice implies, for example, to favour other ethical values over protection of secret information and other intellectual property rights of Agents that are not natural persons.

6.1.1 Privacy

Privacy is “someone's right to keep their personal matters and relationships secret”[71]; it could also be intended as “the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively”[72].

Applying the golden rule, it is a good ethical choice to develop and use SIFIS-Home technologies that allow privacy by design and by default.

6.1.2 Physical safety

SIFIS-Home technologies have interaction with, and produce effects in, the real word; therefore they can damage users and their properties (i.e., cause house fires, damages and even kill a person).

It is therefore a good ethical choice to develop and use SIFIS-Home technologies that protect safety by design and by default.

6.1.3 Security

Security of SIFIS-Home technologies maximises the possibility to protect privacy and safety of users.

It is therefore a good ethical choice to implement SIFIS-Home technologies that provide information security by design and by default.

6.1.4 Control by the user

When use of personal data processed making use of SIFIS-Home technologies is allowed, third parties have access to such personal data and can make decisions about them (becoming data controllers).

[69] Agents is used for natural or legal person, public authority, agency or other body.

[70] See https://en.wikipedia.org/wiki/Golden_Rule.

[71] See https://dictionary.cambridge.org/us/dictionary/english/privacy.

[72] See https://en.wikipedia.org/wiki/Privacy.

Data subjects could be happy with this, but should be informed and should be in the position to make an informed decision about providing access to their personal data.

It is therefore a good ethical choice to implement SIFIS-Home technologies that allow data subjects to make free and aware decisions about providing access to their personal data by design and by default and allow users to maintain control over who and when can process their personal data over time.

6.1.5 Discrimination

When SIFIS-Home technologies implement algorithms, such algorithms can embed bias (this could be the result of deliberate choice or negligence of the developers).

It is therefore a good ethical choice to implement SIFIS-Home technologies that do not suffer from biases by design and by default.

6.1.6 Data commons

Individual dimension of ethical analysis is not enough: the value of personal data is generated through data aggregation.

SIFIS-Home technologies should hinder the processing of personal data when it generates asymmetries of power over such data according to the extractive model (Zuboff, 2019). It is therefore important to design SIFIS-Home technologies that do not foster this. On the other hand, it is useful to design SIFIS-Home technologies in order to foster the generation of value without producing asymmetries of power and therefore generating commons out of the aggregated data. To this end, it is important to maximise the control of individual users and deliberately design technologies that encourage the production of common goods from the aggregation of data carried out on a voluntary basis by users or (where applicable) in application of laws.

6.1.7 Free technologies

If SIFIS-Home technologies are available under free licenses, users (and the public at large) are allowed to scrutinize the functioning of such technologies.

Adoption of free software / open source licenses for software (and adoption of other free licenses for other artifacts) can also foster collaboration and contribution by users (and by the public at large) in the improvement of such technologies.

When the technology is an artificial intelligence system, all information that allows to reproduce and verify the functioning of the algorithm according to the scientific method (including the data that allowed the training of the system, provided that the privacy of the data subjects is respected) should be publicly available to allow users (and the public at large) to scrutinize the functioning of such technologies and collaborate/contribute to their improvement.

Also creative works not consisting in software (like datasets, texts, images and pictures) should be available under free licenses to allow users (and the public at large) to collaborate and contribute in their improvement.

It is therefore a good ethical choice to implement and distribute free technologies.

6.1.8 Trust

Trust in SIFIS-Home technologies by users is positively impacted by technologies that comply with the ethical goals mentioned above.

It is therefore a good ethical choice to implement SIFIS-Home technologies that comply with the above ethical goals to also increase trust in users of the SIFIS-Home technologies, and their adoption, collaborative improvement and public scrutiny.

6.2 *The Agents*

The following considerations are articulated for the different Agents interacting with SIFIS-Home technologies in the light of the objective of maximising the ethical goals to develop and use technologies that protect privacy, are safe and secure, enable control by the users, avoid discrimination, foster the creation of data commons, and are available as free technologies, therefore promoting trust.

6.2.1 Agents that develop SIFIS-Home technologies

Developers should develop SIFIS-Home technologies that maximise the above ethical goals.
Making available information that ease compliance with the above ethical goals, developers can support data controllers and data processors that adopt SIFIS-Home technologies to maximise the achievement of such ethical goals:

- Natural persons that use SIFIS-Home technologies in the course of a purely personal or household activity should adopt technologies that maximise the above ethical goals.
- Natural persons that use SIFIS-Home technologies as data subjects would trust more easily SIFIS-Home technologies that maximise the above ethical goals.
- Agents that use SIFIS-Home technologies as data controllers (including SaaS providers) should adopt SIFIS-Home technologies that maximise the above ethical goals and therefore foster trust by data subjects.
- Agents that use SIFIS-Home technologies as data processors should adopt SIFIS-Home technologies that maximise the above ethical goals and therefore foster trust by data controllers and data subjects.

7 Action points for legal compliance

Considering the EU data protection regulatory framework (GDPR, etc.), also in the light of the CJEU rulings and the EDPB's indications, and the state of the art of the tools available to foster fulfilment of data processing obligations, it is good to implement further tools for Agents involved in the development and use of SIFIS-Home technologies.
Articles 25 and 32, of GDPR, provide to comply to privacy by design and security in processing obligations taking into account the state of the art; therefore, as long as the these tools will constitute an advancement in the state of the art, they would also be beneficial for data processing in IoT at large: they will be a point of reference that other Data Controllers could not avoid to consider because they will be at the forefront of the state of the art.
Considering also the results of the ethical analysis described in chapter 6 and starting from the frame used for such ethical analysis (that considers different categories of Agents), different **dashboards** are proposed as part of SIFIS-Home technologies; such dashboards should allow the different Agents developing and/or using SIFIS-Home technologies to: (i) facilitate compliance to GDPR obligations by data controllers and data processors, and (ii) maximise the power and control by the data subjects.
Dashboard for the Agents that develop SIFIS-Home technologies could include reuse of tools already available that facilitate legal compliance in case of reuse of software available according to the terms of free software / open source licenses.
The following dashboards are proposed for the different categories of Agents and for each of them it is indicated the list of possible functions available.

7.1 *Dashboard for Agents that develop SIFIS-Home technologies*

The dashboard for Agents that develop SIFIS-Home technologies could be available as part of the developing tools and, as way of example, should allow the developer to reply to the following questions, allowing them to get a review based upon the traffic light system indicated in chapter 4.3 (Legal guidelines) of D2.2 Preliminary Developer guidelines:

1. Did you analyze the information to be used by the data controller for compliance to articles 13, 14, 25 and 32 of GDPR?
2. Does the document containing the information to be used by the data controller for compliance to articles 13, 14, 25 and 32 of GDPR accompanies the software? Is it available at request of data controllers?

3. Did you successfully perform a Privacy Impact Assessment based on reasonable assumptions for at least a standard use case?
4. Does the documentation of the Privacy Impact Assessment accompany the software? Is it available at request of a data controller?
5. Did you follow the OpenChain specification or other public specification for licensing compliance?
6. Do the compliance artifacts that show licensing compliance accompany the software? Are they available at request of an Agent that wants to distribute or make available the software?
7. The methodology used and the standard followed in creating the document containing the information to be used by the data controller for compliance to articles 13, 14, 25 and 32 of GDPR, the privacy impact assessment, and the compliance artifacts, is publicly available, free of any right of third party, so that everyone can assess compliance and use it?

Concerning question 1, provision of the information to be provided to the data controller for compliance to articles 13, 14, 25 and 32 of GDPR could be facilitated providing a tool that allows the provision of such information by the software developer:

1. What categories of personal data is processed by the software application?
2. For each category of personal data that is processed by the software application, is it:
    1. pseudonymized?
    2. Anonymized?
    3. Stored locally?
    4. Stored for how long?
    5. Accessible and/or to be communicated to third parties?

Concerning question 3, provision of the information to the Data Controller for performing a PIA could be facilitated adopting a tool that allows the provision of the information required for the PIA of IoT devices of CNIL[73].

Concerning question 5, provision of the information to the Data Controller for elaborating the compliance artifacts could be facilitated by adopting some of the tools indicated in chapter 4.

The dashboard of the software developers could work allowing to automatically retrieve from the development tools some of the information required, at least as a proposed answer to the fields to be filled in (as way of example, listing the categories of data processed by the application developed).

7.2 *Dashboard for Agents that use SIFIS-Home technologies as Data Controllers*

The dashboard for Agents that use SIFIS-Home technologies to process personal data as Data Controllers could include different sections:

1. data from software developers;
2. data to/from Data Subjects;
3. data to/from Data Processors.

Section 1 (data from software developers) should allow Data Controllers to receive data uploaded by software developers.

[73] See https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

Section 2 (data to/from data subjects) should allow Data Controllers to:

1. input name, address, and contact details;
2. fill in the PN for the Data Subjects;
3. receive consent from the Data Subjects;
4. exchange communications with Data Subjects.

Section 3 (data to/from Data Processors) should allow Data Controllers to:

1. input name, address, and contact details;
2. exchange contract or other legal act according to art. 28, of GDPR with Data Processors;
3. exchange information (and, where applicable, appropriate data protection clauses) about where (if in EU or, if extra EU, in which country) the data will be transfered;
4. exchange communications with Data Processors.

It could be useful to implement the dashboard for Agents that use SIFIS-Home technologies as Data Controllers in 2 different situations:

1. dashboard for Data Controllers that upload applications into the SIFIS-Home market place, and
2. dashboard for Data Controllers that use applications uploaded into SIFIS-Home market place by third parties.

7.2.1 Data Controllers that upload applications into SIFIS-Home market place

The dashboard for Agents that upload applications into SIFIS-Home market place applies, as way of example, to Software as a Service (SaaS) providers that make their service available through applications uploaded in the SIFIS-Home market place.
Failure to properly fill in this dashboard could prevent the possibility to upload the application in the SIFIS-Home market place.

7.2.2 Data Controllers that use applications uploaded into SIFIS-Home market place by third parties

The dashboard for Agents that use applications uploaded into SIFIS-Home market place by third parties applies, as way of example, to home users that do not use SIFIS-Home technologies solely for personal or household activities.
Home users should have the option to fill the dashboard described above.

7.3 *Agents that use SIFIS-Home technologies as Data Processors*

Agents that upload applications into SIFIS-Home market place (as way of example, SaaS providers that make their service available through applications uploaded in the SIFIS-Home market place) could opt to not be Data Controllers but Data Processors.
If this is the case, they would sign with the Data Controllers that use their applications agreement conforming to article 28, of GDPR.
The dashboard for Data Processors should include different sections:

1. data from software developers;
2. data to/from Data Controllers.

Section 1 (data from software developers) should allow Data Processors to receive data uploaded by software developers.
Section 2 (data to/from data controllers) should allow Data Processors to:

1. input name, address, and contact details;
2. exchange contract or other legal act according to art. 28, of GDPR with Data Controllers;
3. exchange information (and, where applicable, appropriate data protection clauses) about where (if in EU or, if extra EU, in which country) the data will be transfered;
4. exchange communications with Data Controllers.

7.4 *Dashboard for natural persons that use SIFIS-Home technologies in the course of a purely personal or household activity*

Natural persons that use SIFIS-Home technologies in the course of a purely personal or household activity could use applications that do not send personal data outside of the house to third parties or applications that send personal data to third parties. Third parties could process personal data as Data Controllers or as Data Processors.

The dashboard for natural persons that use SIFIS-Home technologies in the course of a purely personal or household activity should include different sections:

1. data from software developers;
2. data to/from Data Controllers;
3. data to/from Data Processors.

Section 1 (data from software developers) should allow Data Processors to receive data uploaded by software developers.

Section 2 (data to/from Data Controllers) should allow the users to:

1. receive PNs from Data Controllers;
2. send consent to Data Controllers;
3. exchange communications with Data Controllers.

Section 3 (data to/from data processors) should allow users to:

1. exchange contract or other legal act according to art. 28, of GDPR with Data Processors;
2. exchange information (and, where applicable, appropriate data protection clauses) about where (if in EU or, if extra EU, in which country) the data will be transfered;
3. exchange communications with Data Processors.

7.5 *Further action points*

Implementation of some general characteristics could be evaluated for all the dashboards and their content. The dashboards should:

1. allow storage of content;
2. allow addition and exchange of further pledges, particularly, pledges that foster generation of commons out of the aggregation of personal data;
3. allow the exercise of any further rights (e.g. access to data generated by IoT devices[74]);

[74] See art. 4 of the proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act) of 23.2.2022on harmonised rules on fair access to and use of data (Data Act) of 23.2.2022 COM(2022) 68 final - https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data).

4. be organized and allow easy search and easy actions (as way of example, a data subject could be allowed to revoke all consents provided to different, including all, Data Controllers with one click);
5. provide irrefutable evidence of communications sent by Data Controllers and Data Processors.

In the further course of the project, it might be useful to assess whether an ontology is available that could be successfully used to facilitate the development of dashboards functionalities and, if it's not available, to develop it by identifying the semantic domain from the information available in Annex 1.

8 Conclusion

This deliverable presents the results of the legal analysis performed; in particular, chapter 2 provides the results of the analysis relating to the protection of personal data and chapter 4 provides the results of the analysis relating to compliance with the obligations imposed by free software / open source licences.

Chapter 6 provides the results of the ethical analysis of SIFIS-Home technologies.

The analysis performed leads to the conclusion that it is advisable to implement tools that favour legal compliance and maximise user control following emerging practises in the field.

In order to achieve these results and, at the same time, improve the state of the art, SIFIS-Home could reuse some of the existing tools:

1. tools concerning compliance with GDPR obligations described in chapter 3, and
2. tools concerning compliance with obligations provided by free software / open source licenses described in chapter 5.

In chapter 7 some action points are presented to design some dashboards that reuse tools already available and add further tools to SIFIS-Home technologies.

9 References

[Article 29 WP, 2017] Article 29 Working Party (2017), “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”, April 4 2017, Accessed February 20, 2022, https://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[Allhoff et al., 2022] Allhoff, F., & Henschke, A. (2018), “The Internet of Things: Foundational ethical issues”, Internet of Things, Volumes 1–2, September 2018, Pages 55-66. Accessed February 15, 2022.
https://www.sciencedirect.com/science/article/pii/S2542660518300532

[Antoniou et al., 2019] Antoniou, J., & Andreou, A. (2019), “Case Study : The Internet of Things and Ethics” ORBIT Journal, 2(2), 2019. Accessed February 19, 2022.
https://doi.org/10.29297/orbit.v2i2.111

[Bain, 2010] Bain, M. (2010). “Software Interactions and the GNU General Public License” International Free and Open Source Software Law Review, 2-2 (2010). Accessed February 15, 2022. http://www.ifosslr.org/ifosslr/article/view/44

[Chen et al., 2020] Chen, J., & Edwards, L., & Urquhart, L., & McAuley, D. (2020) “Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exception”, International Data Privacy Law, 10-4, November 2020.

[EDPB. 2019] European Data Protection Board Plenary Meeting, “Guidelines 3/2019 on processing of personal data through video devices”, EDPB Guidelines (2019, accessed 20 February 2022. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf,

[Fontana et al., 2008] Fontana, R, & Kuhn, B. M., & Moglen, E., & Norwood, M., & Ravicher, D. B., & Sandler, K., & Vasile, J., & Williamson, A. (2008). A Legal Issues Primer for Open Source and Free Software Projects, Accessed February 19, 2022.
http://softwarefreedom.org/resources/2008/foss-primer.pdf

[Hemel et al., 2017] Hemel, A., & Coughlan, S. (2017), Practical GPL Compliance. San Francisco, CA: Linux Foundation, 2017

[Kuhn et al., 2008] Kuhn, B. M., & Sebro, A. K. Jr., & Gingerich, D., & Free Software Foundation, Inc., & Software Freedom Law Center (2008). Copyleft and the GNU General Public License: A Comprehensive Tutorial and Guide, 2008 Accessed February 19, 2022.
https://copyleft.org/guide/

[Meeker, 2017] Meeker, H. (2017). Open source for business. A practical guide to open source licensing. North Charleston SC: Createspace Independent Publishing Platform, 2017

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

[Rosen, 2005] Rosen, L. (2005). Open source licensing: software freedom and intellectual property law. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference, 2005

[Zuboff, 2019] Zuboff, S. (2019). The age of surveillance capitalism: the fight for the future at the new frontier of power. Public affairs, 2019

Glossary

Acronym	Definition
GDPR	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)
PIA	Privacy impact assessment
PN	privacy notice
SIFIS-Home	Secure Interoperable Full Stack Internet of Things for Smart Home

Annexes

1 *List of labels for GDPR compliance*

LABEL	NATURE	DEFINITION	SOURCE
anonymisation	Action	is a technique applied to personal data in order to achieve irreversible de-identification. Therefore, the personal data must have been collected and processed in compliance with the applicable legislation on the retention of data in an identifiable format.	Recital 26, GDPR
consent (of the data subject)	Action	means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her	Art. 4 (11) GDPR
data controller	Agent	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;	Art. 4 (7) GDPR
data minimization	Action	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	Art. 5 (1.C) GDPR
data processor	Agent	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Art. 4 (8) GDPR
data recipient	Agent	means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.	Art. 4 (9) GDPR
data storage limitation	Action	personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed	Art. 5(1), point e, GDPR
data subject	Agent	an identified or identifiable natural person on whom data are referred	Art. 4.(1) GDPR
Encryption and other mitigation measures	Action	In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.	Recital 83, GDPR
pseudonymisation	Action	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and	Art. 4 (5) GDPR

		organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person	
third party	Agent	means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data	Art. 4 (10) GDPR