D2.7

Final Report on Legal and Ethical Aspects

SIFIS-Home
Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/03/2023
Actual submission date: 31/03/2023

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

31/03/2023
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)

Approved by: Giles Brandon (IC), Göran Selander (ERI)

Revision History

Version	Date	Name	Partners	Section Affected Comments
0.1	15/12/2022	Defined ToC	POL	All
0.2	25/01/2023	UPGRADE 1	POL	All
0.3	10/02/2023	UPGRADE 2	POL	All
0.4	20/02/2023	First version	POL	All
0.5	28/02/2023	Second version	POL	All
0.6	02/03/2023	Updates	POL	All
0.7	05/03/2023	Updates	POL	All
0.8	15/03/2023	Updates	POL	All
0.9	21/03/2023	Updates	POL	All
1.0	31/03/2022	Ready for submission	POL	All

Executive Summary

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

It analyses two 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 in 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 that are implemented in a pilot tool included in the SIFIS-Home technologies - the privacy dashboard - that facilitates 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 analyses 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 in 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 has adopted this approach by 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 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 rules. Therefore, it is primarily those who use the software to process personal data or obtains personal data through its use, who have to be certain that their usage of the 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:

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*".

- 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
- protect data by design and by default pursuant to Article 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 does not 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 Article 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 decides the purposes and means of processing 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 are called Joint Controllers.

5 Article 4 (1), GDPR

6 Art. 4 (6), GDPR

The Data Controller will be the subject responsible for the correct processing of personal data.

There are different obligations that the GDPR imposes on 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 to SIFIS-Home technologies:

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

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"

- providing 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] obliges the Data Controller to implement appropriate technical and organisational measures for ensuring privacy "by default".
Article 32[11] requires the Data Controller 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 detail 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

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.

considered as a Controller in respect of that processing and will have the same liability as a Data Controller[13].

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).

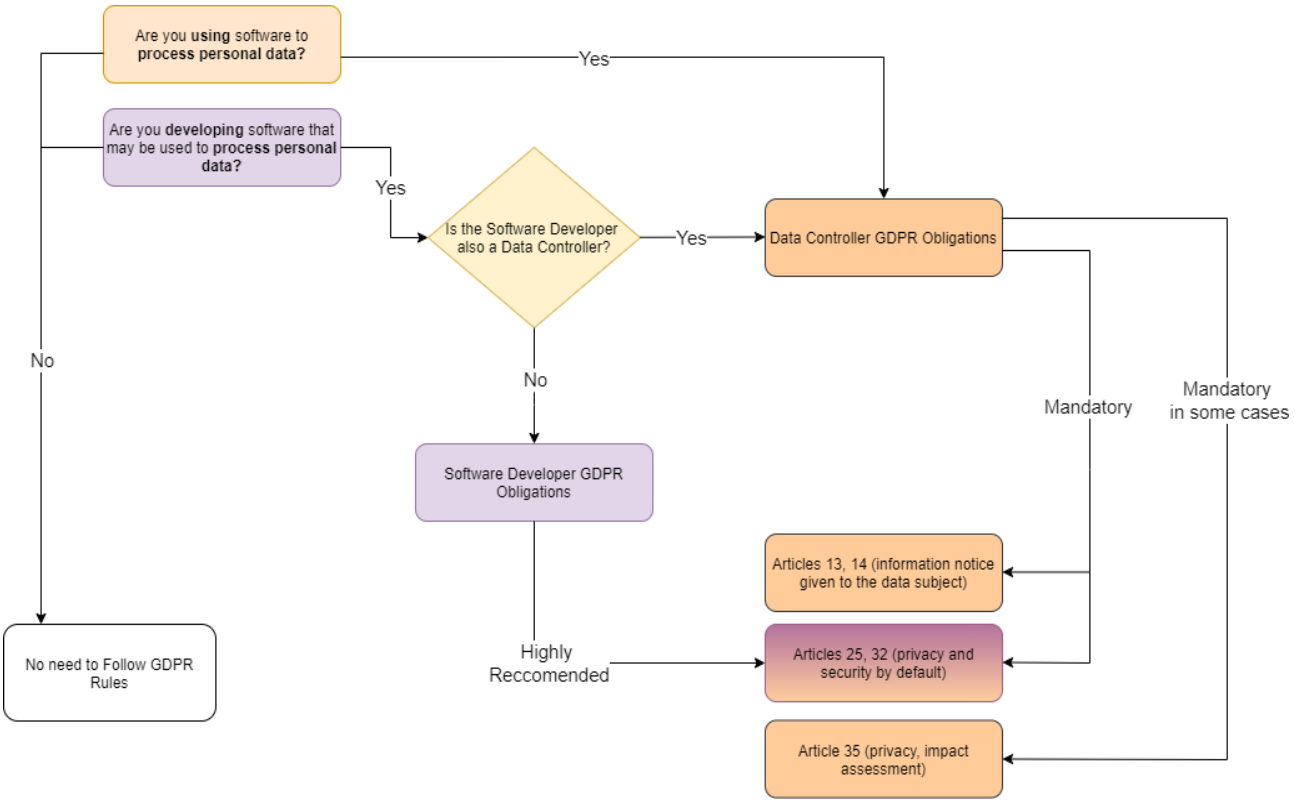
The software developer **may or may not be Data Controller himself.** He/she becomes a Data Controller when they themselves use such a software to process personal data. But, regardless of whether he/she is or is not a Data Controller, he/she has interest to follow GDPR Articles 25 and 32, and to provide 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 Articles 13, 14, 25**,** 32 and 35.

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.



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

Getting a certain software to be GDPR-compliant is no easy task and it cannot be done exclusively by the software designer, nor can it 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 process 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 with the GDPR requires "*appropriate technical and organizational measures*", something which is only partly obtained through what has 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*

14 Available at https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/

processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features[15]".

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 dentist's 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 to be compliant with this GDPRs requirements[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.

15 Recital 78, GDPR

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 must be done is to define 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 software developers are often not just individuals, but are part of a larger structure, such as a software company.

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.

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 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 consider 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 the 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 thorough 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 consider these issues.

Then, it should also offer state-of-the-art ways to process personal data in a secure and privacy conscious way ensure that Data Controllers (including home-owners that choose to process personal data as Data Controllers) can comply with GDPR, and ensure that Data Subjects are able to effectively exercise their right 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 is a reasonable option to provide for the possibility that the home-owner makes his decision about whether to comply 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 Privacy Notice requirements into two types: stylistic requirements and content requirements.

Regarding the stylistic requirements, the PN must be:

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

- 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.
- 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 exist to help 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.

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":

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
28 CNIL, *Privacy Impact Assessment Methodology*, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

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.

By "special categories of data", the GDPR means information that is especially sensitive and is concerned with peculiar traits or conditions of the individual, such as their 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 always lies with the Data Controller.

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 with the GDPR. The French CNIL[35] created a useful tool[36] that has quickly become the reference standard. Using

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/

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

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 as it was in regard 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 recommended that software developers make available as much useful information for performing a PIA as possible, thereby aiding the subsequent Data Controller to comply with Article 35 of the 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 is presented to aid both software developers and general Data Controllers in managing which information has to be given to the Data Subjects. 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 tool 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.

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.

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

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

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.

software cannot exclude that that software interferes with a patent-protected invention. The use and diffusion of free software is thus also affected by patent law. In some free software licenses, various techniques are used to limit patent interference with free software and to discourage who wants to prevent the use and distribution of free software by claiming a patent. For example, some licenses provide that whoever contributes to the software and/or who distributes it (as the case may be) licenses its (if any) patent rights.

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 analyse 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 is 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.

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.

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

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).

More recently, the DBOM project[55] provided a Digital Bill of Materials (DBoM) to facilitate attestation sharing between organizations, including tools to achieve the goal.

The Linux Foundations supports also the OpenChain Project[56], 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 the OSS Review Toolkit (ORT)[57] was recently presented, which 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[58] 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[59].
Reuse Software project[60] 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[61] project, that aims to support projects in clearly describing their projects, the licenses adopted and security vulnerabilities[62].

Other useful tools are:

- Ninka, a license identification tool[63];
- Open-source License Checker, a license identification tool[64];
- Tern, a tool that generates a software Bill of Materials for container images and Dockerfiles[65];
- Hermine[66] is a tool to manage bill of materials of software components, their licenses and their respective obligations.

53 See https://compliance.linuxfoundation.org/.
54 See https://spdx.dev/ids/.
55 See https://dbom.io/.
56 See https://www.openchainproject.org/.
57 See https://github.com/oss-review-toolkit/ort.
58 See https://www.fossology.org/.
59 See https://github.com/nexB/scancode-toolkit.
60 See https://reuse.software/.
61 ClearlyDefined was also proposed in D2.2 as one of the possible solutions to obtain a "green light" regarding privacy and security compliance.
62 See https://clearlydefined.io/about.
63 See http://ninka.turingmachine.org/.
64 See https://sourceforge.net/projects/oslc/.
65 See https://github.com/tern-tools/tern.
66 See https://gitlab.com/hermine-project/hermine.

Regarding creative works beyond software (e.g. 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[67] and provides information about license attribution[68].

For datasets, it is worth mentioning the licensing assistant made available by the European Data Portal[69].

6 Ethical analysis

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

The Agents[70] 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[71] "*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 highlighting that this choice implies, for example, favouring other ethical values over protection of secret information and other intellectual property rights of Agents that are not natural persons.

6.1.1 Privacy

67 See https://creativecommons.org/choose/.
68 See https://wiki.creativecommons.org/wiki/Best_practices_for_attribution.
69 See https://www.europeandataportal.eu/en/content/show-license.
70 Agents is used for natural or legal person, public authority, agency or other body.
71 See https://en.wikipedia.org/wiki/Golden_Rule.

Privacy is "*someone's right to keep their personal matters and relationships secret*"[72]; 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*"[73].

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, damage 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

By ensuring the security of SIFIS-Home technologies, it helps to protect the 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 the use of personal data processed by SIFIS-Home technologies is allowed, third parties have access to such personal data and can make decisions about them (by becoming data controllers).

Data subjects may be happy with this but should be informed and should be in a 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 when and who 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 the application of laws.

72 See https://dictionary.cambridge.org/us/dictionary/english/privacy.

73 See https://en.wikipedia.org/wiki/Privacy.

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.

The 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 to their improvement.

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

6.1.8 Disadvantaged people

SIFIS-Home technologies could be used by natural persons that are disadvantaged people (minors, or other). Providing for functionalities that allow to protect disadvantaged people (like parental control to protect minors) is a good ethical choice and should be considered in the design of SIFIS-Home technologies.

6.1.9 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.

By making available information that eases 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 thereby foster trust among 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 the 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 cannot avoid considering 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.

The 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 with Articles 13, 14, 25 and 32 of GDPR?
2. Does the document containing the information to be used by the data controller for compliance with Articles 13, 14, 25 and 32 of GDPR accompany 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 upon 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 upon 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, the provision of information from the data controller for compliance with Articles 13, 14, 25 and 32 of GDPR could be facilitated by providing a tool that offers such information from 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 by adopting a tool that offers the information required for the PIA of IoT devices of CNIL[74].

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.

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;

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

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

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

7.2.1 Data Controllers that upload applications into SIFIS-Home marketplace

The dashboard for Agents that upload applications into the SIFIS-Home marketplace applies, by way of example, to Software as a Service (SaaS) providers that make their services available through applications uploaded in the SIFIS-Home marketplace.

Failure to properly fill in this dashboard could prevent the possibility to upload the application in the SIFIS-Home marketplace.

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

The dashboard for Agents that use applications uploaded into the SIFIS-Home marketplace by third parties applies, by 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 the SIFIS-Home marketplace (as way of example, SaaS providers that make their service available through applications uploaded in the SIFIS-Home marketplace) 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 Article 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 transferred;
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 transferred;
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[75]);
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 is not available, to develop it by identifying the semantic domain from the information available in Annex 1.

8 Implementation of the Privacy Dashboard

The General Data Protection Regulation is designed to protect the personal data of EU citizens and give them more control over their personal information, by imposing a series of requirements to the *data controllers*, the individuals who process personal data, and consequentially giving a number of rights to the *data subjects*, the individuals whose data is processed.
We believe that by providing a user-friendly privacy dashboard that allows data subjects to easily access and control their personal data this concept will be easier to embrace. By making it simple and straightforward for individuals to exercise their rights, such as the right to access their personal data or the right to have their data erased, they would be more likely to do so.

75 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).

However, a privacy dashboard such as the one that will be presented throughout the document alone may not be enough to promote positive behavior change. Data controllers, as well as their habits, also play a critical role in ensuring that GDPR-mandated rights are upheld and data subjects' rights are respected. As such, there is a need for data controllers to voluntarily or be obliged by law to use new technologies that facilitate GDPR compliance and promote data protection.

One way to achieve this could be through industry standards. A well-made and complete privacy dashboard has the potential to become the industry standard by offering a comprehensive, easy to use solution for managing personal data in compliance with GDPR requirements. The objective would be to get more and more data processors to adopt this technology, achieving a ripple effect.
If the concept of a privacy dashboard starts to be discussed, proposed and implemented, some of the legal arguments deriving from that discussion could foster the change of the status quo and produce incentives for its adoption.

Particularly,

- GDPR Article 12.1 "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and **easily accessible form**, using clear and plain language, in particular for any information addressed specifically to a child*";
- GDPR Article12.2 "*The **controller shall facilitate the exercise of data subject rights under Articles 15 to 22**. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.*".

The role of the state of the art in the design of privacy by design systems could help in this. According to GDPR Article 25 "***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.*".

If tools such as the privacy dashboard represent an advancement in the state of the art, they could even become mandatory.

For example, under the current EU legislation, websites must obtain users' consent before using cookies or other tracking technologies, unless the use of cookies is strictly necessary for the operation of the website. This requirement has led many websites to implement cookie banners or pop-ups that ask users to consent to the use of cookies. Until recently, the rules and guidelines of the authorities did not require any particular requirements for banner cookies. They were therefore designed in such a way as to maximise user acceptance: refusing consent was complicated (or even impossible). Then the EDPB and the European data protection authorities called for more stringent requirements (see EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities adopted on 12 March 2019). This has made it easier to refuse consent to cookies (nudging effect).

Nudging can be a powerful tool for promoting compliance with legal requirements and encouraging pro-social behaviors, by taking advantage of people's natural biases and tendencies.

The privacy dashboard shows what could be done: fostering the adoption of best practices to controllers in order to make it easier for data subjects to exert their rights.

According to GDPR every data processing requires the delivery of a *Privacy Notice* from the data controller to the data subjects. Therefore, a privacy dashboard that lists all the privacy notices can also provide a centralized and easily accessible view of all the notices themselves that have been created and shared with data subjects. This can help data controllers ensure that they are providing GDPR-compliant privacy notices to data subjects about how their personal data is being collected, used, and shared. This clear and transparent view of their data processing activities may help, through “nudging”, in building trust with data subjects and regulators by demonstrating that the organization is committed to transparency and accountability.

Another way that nudging is incorporated into the dashboard for the data controller is through visual cues, such as displaying a red "warning" symbol when a data processing activity appears to be non-compliant with GDPR requirements. This can alert data controllers to potential issues and encourage them to take corrective action and is present in the dashboard through the traffic light system, indicated in Chapter 4.3 (Highlights) of D2.4 Final Developer guidelines, and implemented as a feature which we will discuss in more detail later.

The privacy dashboard is conceived as a unified manager of privacy information and communication tools, but it is important to highlight that it can be implemented as a distributed and federated network of instances that communicate among them; thereby every Agent can choose where to have his instance of the privacy dashboard and have full control of his data.

This chapter describes the part of the privacy dashboard that refers to interactions among the controller and data subjects (Chapter 7 provides also for a dashboard for developers of SIFIS-Home applications and data processors).

For data subjects, a privacy dashboard can empower them in exercising their rights and improving their knowledge of their current privacy situation. For example, data subjects could access the dashboard and review the privacy notices they have accepted at any time to understand what kind of data is being collected, how it is being used, and who it is being shared with. This can help data subjects to make informed decisions about whether to provide their personal data, request access to it or to relinquish their consent.

It could therefore be useful to both data controllers and data subjects to have a single digital space that allows them to access and view, at a single glance, all the information they need in order to ensure compliance with GDPR or to exercise their rights.

By having all this information in one place, a data controller can easily identify any potential GDPR compliance issues. For example, if a retention period for certain data is about to expire, the data controller can take pre-emptive action to either delete the data or try to extend the retention period, informing the data subject. The dashboard includes prompts to remind data controllers to obtain explicit consent for certain types of data processing activities, or to conduct regular data protection impact assessments. These prompts can be designed, again, to “nudge” data controllers to take actions.

A dashboard for data subjects can also be a useful tool for ensuring compliance with the GDPR. The GDPR gives data subjects certain rights, such as the right to access their personal data, the right to have

their personal data corrected, and the right to have their personal data deleted. A dashboard for data subjects can provide a user-friendly interface that allows individuals to exercise these rights and manage their personal data. This can streamline the process of answering to the requests of data subjects and help data controllers comply with the GDPR more efficiently.

All of this is even more true in the case of Smart Home Devices, such as those that will refer to the SIFIS-Home framework. These devices, already usually positioned in risky environments, such as private homes of individuals, typically collect and process a large amount of personal data, including location data, audio and video recordings, and sensor data.

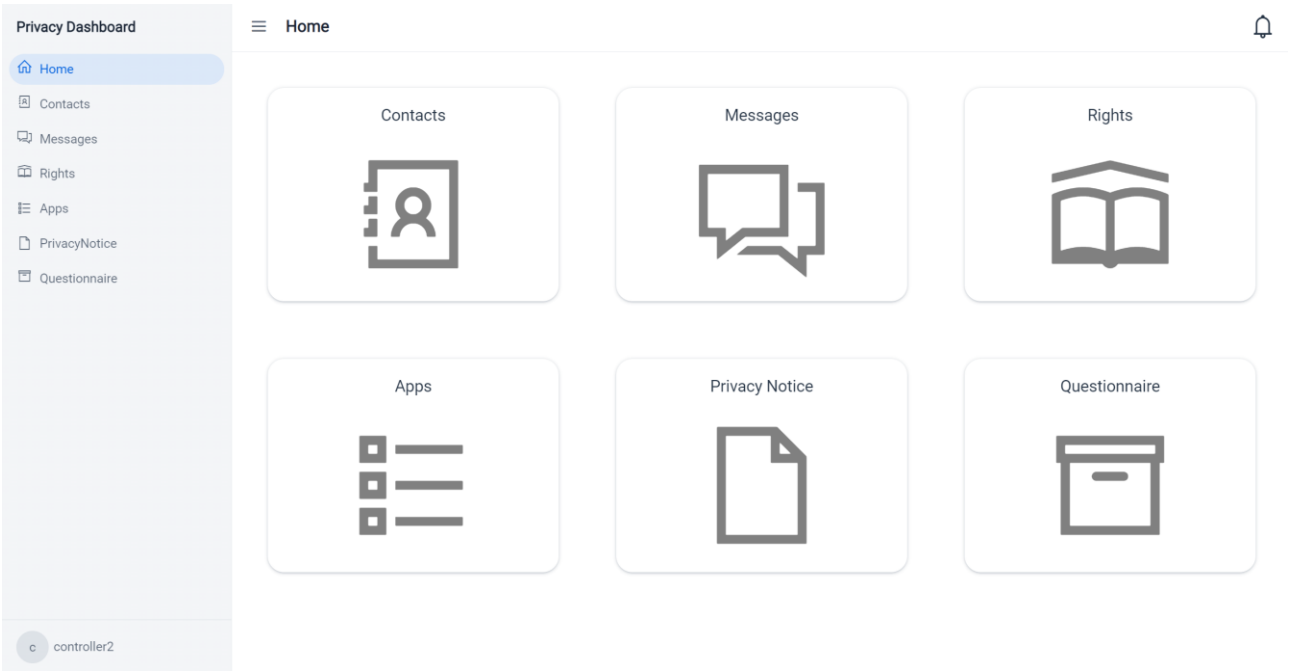
It is for this reasons that we aimed to create a Privacy Dashboard capable of displaying information about the types of personal data being processed, such as the legal basis for processing that data, the retention periods for that data, and potentially to even rate the measures in place to protect the data from unauthorized access, breaches, or unlawful use.

In Chapter 7 (Action points for legal compliance), we defined such a dashboard as a tool that refers to different Agents developing and/or using SIFIS-Home technologies to: (i) facilitate compliance to GDPR obligations by data controllers and data processors, and (ii) increase the power and control by the data subjects.

The privacy dashboard shows that further "nudging" could be fostered to protect data subject rights.

In this chapter, the dashboard will be analysed from the perspective of the Data Controller and the Data Subject, offering a point-by-point analysis of each of its features.

8.1 *The Privacy Dashboard in general for Data Controllers*



The privacy dashboard's main page from the perspective of a Data Controller.

From the perspective of a Data Controller, the dashboard can provide a range of detailed features to help them ensure compliance with the GDPR, some of which are strictly connected to those of the Data Subject, which will be described in the following chapters.

For data controllers, such a privacy dashboard:

- Provides a list of all privacy notices: This can include all the privacy notices that have been created and shared with the data subjects. Data controllers can use this information to ensure that they are providing accurate and up-to-date information to data subjects about how their personal data is being collected, used, and shared.
- Allows the data controller to obtain at first glance a list of all the data subjects whose data is being processed by the data controller themselves. This can be of help in contacting the data subjects, should the need arise, and track their requests.
- Offers a clear view on data retention periods: this can include information on the specific retention periods for different types of data, as well as potential methodologies for quickly and securely disposing of data once the retention period has expired. This can help data controllers to ensure that they are only keeping data for as long as it's necessary and that the data is deleted or anonymized when the retention period expires.
- Tracks data subject rights requests and their status. This includes a log of all data subject access requests, correction requests, and deletion requests, as well as the status of each request, such as whether it has been approved or denied. Data controllers can use this information to manage and respond to data subject rights requests in a manner compliant to what's provided by the GDPR.
- Allows data controllers to quickly contact and/or be contacted by data subjects for any kind of request any of them may have.

The dashboard also offers a questionnaire that the data controller should complete in order to get a quick assessment of its compliance with GDPR. This questionnaire asks the data controller to answer some questions regarding the ways in which personal data is being processed, both technical and conceptual. For example, it asks whether there is an automatic mechanism that deletes personal data after the chosen period of time, if there is any data transfer to third parties, or if there is any kind of encryption for personal data. The answers the data controller gives are rated in a traffic light system, with privacy-compliant answers coming up in green, not entirely compliant answers in yellow, and not compliant answers in red. Through this questionnaire, the data controller is advised to exercise more or less caution in employing their methods of data processing and facilitates them to change some of the methodologies in order, at least, not to have any red answers.

The traffic light system is also useful to assess GDPR and software license compliance for software developers who build software based on the SIFIS-Home architecture.

Through a series of questions, the system scores the software based on different criteria:

- Whether he has successfully performed a Privacy Impact Assessment;
- Whether he has produced enough information for compliance to articles 13, 14, 25 and 32 GDPR;
- Whether he has followed some specification for its software, such as OpenChain, and if so, whether the software is accompanied by the relative compliance artifacts;
- Whether the methodology followed for the data processing is publicly available.

If the data controller scores positively on all the questions, the dashboard shows him a green light to symbolize that he is able to easily assess the GDPR compliance of the software and compliance with the software licenses. If some requirements are satisfied only partially, the data controller gets a yellow light that tells that the software *should* be GDPR and software license compliant, but caution is needed as not all the recommended characteristics are met.

Finally, a red light is shown if one or more of the features are missing or incomplete. This does not mean that the software is definitely not GDPR compliant, rather, it advises the software developer to carefully analyze it.

8.2 *Current status of dashboard feature implementation*

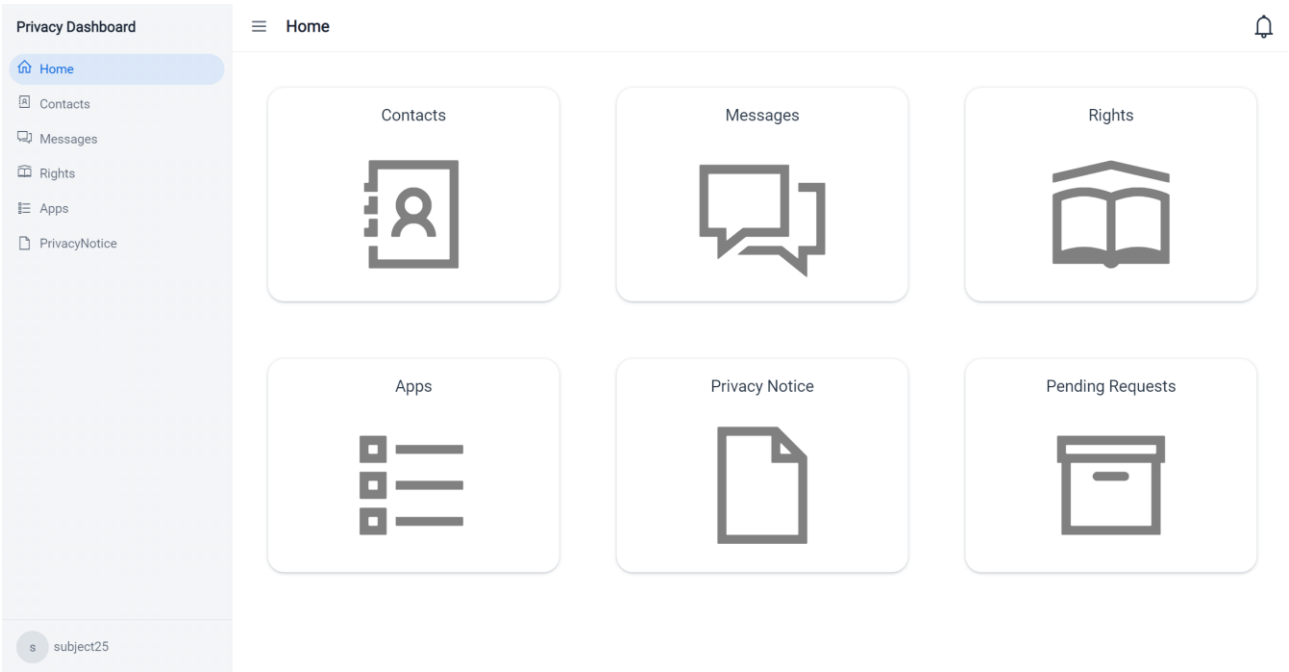
Before moving on with the analysis of the single features of the dashboard, which is now in its prototype state, it is important to notice that it aims to implement the features and objectives described in Chapter 7 (Action points for legal compliance). The majority of these features, along with their original recommendations, have been successfully implemented.

In Chapter 7 (Action points for legal compliance) we propose different dashboards for different roles: one for the data subject, another for the data controller, and so on. The dashboard has access to different features inside its sub-menus.
The "traffic light system", indicated in Chapter 4.3 (Legal guidelines) of D.2.4, was implemented, from the perspective of the data controller, in the "questionnaire" view that will be analysed later. The questions both focus on topics which are more strictly related to privacy and GDPR compliance, and on open software compliance specifications and good practices, such as the OpenChain specification.

The dashboard shows data coming from different categories of subjects: software developers, data subjects and data controllers. It is possible to show the input name, address and contact details of each of them, if they have of course given their consent, and it is possible for data controller and data subject to quickly and easily communicate between them.

The information shown differs from subject to subject. Each agent can only see the details of people relevant to exercise their rights and for GDPR compliance.

8.3 *The Privacy Dashboard in general for Data Subjects*



The privacy dashboard's main page from the perspective of a Data Subject.

As already mentioned, the GDPR gives data subjects certain rights, such as the right to access their personal data, the right to have their personal data corrected, and the right to have their personal data deleted. From the perspective of the data subjects, the dashboard provides a user-friendly interface that allows individuals to exercise these rights and manage their personal data.

For data subjects, such a dashboard allows to:

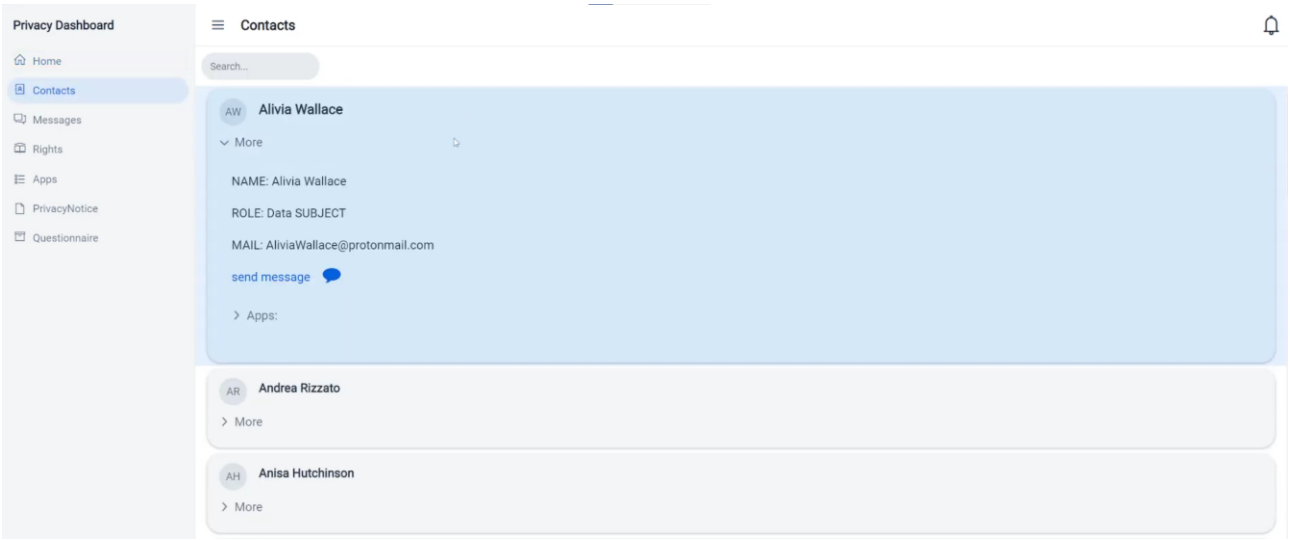
- Provides a list of all privacy notices: this can include all the privacy notices that have been created and shared with the data subject. Through them, the data subjects gain immediate information on how their personal data is being processed by different data controllers, for how long, who those data controllers are and how can they contact them.
- View and access their personal data: providing a view of what personal data an organization holds about them, and how it is being used, shared and retained.
- Request corrections to their data. If a data subject believes that the data held about them is incorrect, they have the right to request that it be corrected. A dashboard can allow individuals to easily request corrections and track the status of their requests.
- Request deletion of their data. Data subjects have the right to request that their personal data be deleted, or to withdraw their consent. The dashboard enables individuals to request that their data be deleted and, again, track the status of their requests.
- Monitor and control data sharing: the dashboard enables data subjects to view and manage the sharing of their data, giving them more control over how their data is used.

Such a dashboard allows a streamlining of requests coming from data subjects, automating them and providing the subjects themselves with an immediate view of how their personal data is being used. This in turns allows data controllers and entire frameworks, such as SIFIS-Home, to build trust with their customers and demonstrate their commitment to data privacy.

8.4 *The Contacts View*

The "Contacts" view on the dashboard enables easy communication and feedback between data controllers and their data subjects, allowing for a more transparent and collaborative approach to data processing. This would not only help data controllers remain compliant with GDPR requirements, but also strengthen trust between them and their data subjects.

8.4.1 For Data Controllers



The Contacts view for the Data Controller.

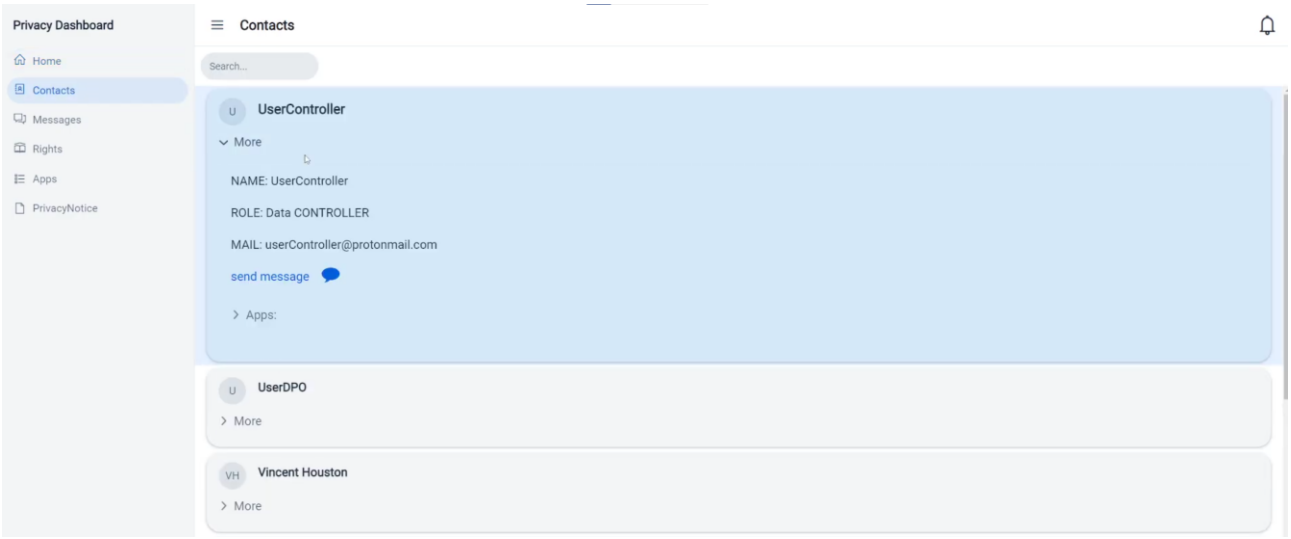
The “Contacts” view of the privacy dashboard enables **data controllers** to view a list of all the data subjects with whom they have interacted and send them updates, notices, and other important information. The view is integrated with a messaging system that allows data controllers to send text messages to their data subjects, providing updates on data processing activities or on requests.

The dashboard could be used to notify data subjects about data breaches, privacy policy updates, and other important information. The data controller could send notifications directly to data subjects through the dashboard, allowing for timely and efficient communication.

For example, if a data controller decides to change its privacy policy, it could use the messaging system to inform its data subjects and request their consent to the updated policy.

The "Contacts" view on the dashboard aims to provide a valuable tool to communicate with data subjects in a transparent and efficient way. The ability to conveniently manage and respond to data subject requests and inquiries would improve the data controller's compliance with GDPR obligations and enhance trust between the data controller and data subjects.

8.4.2 For Data Subjects



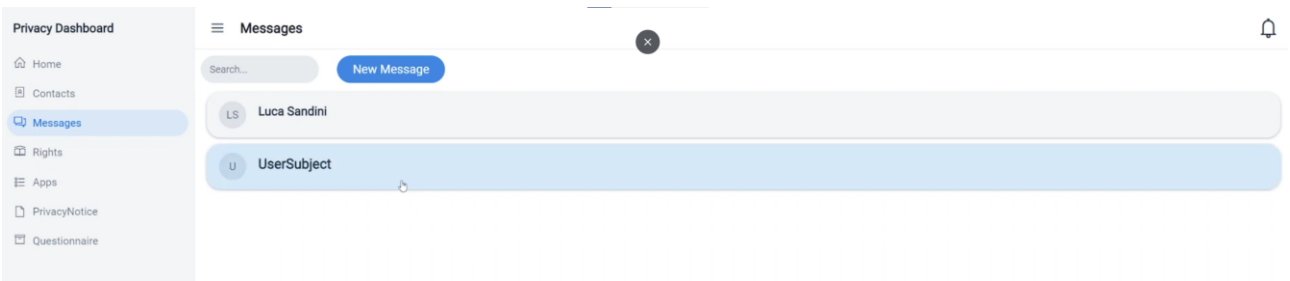
The Contacts view seen by the Data Subject.

For **data subjects,** the view enables them to quickly view all of the data controllers to whom they have provided their personal data. For each data controller, the dashboard would display relevant information related to the application the data subjects are using, such as their contact details and their privacy policy.

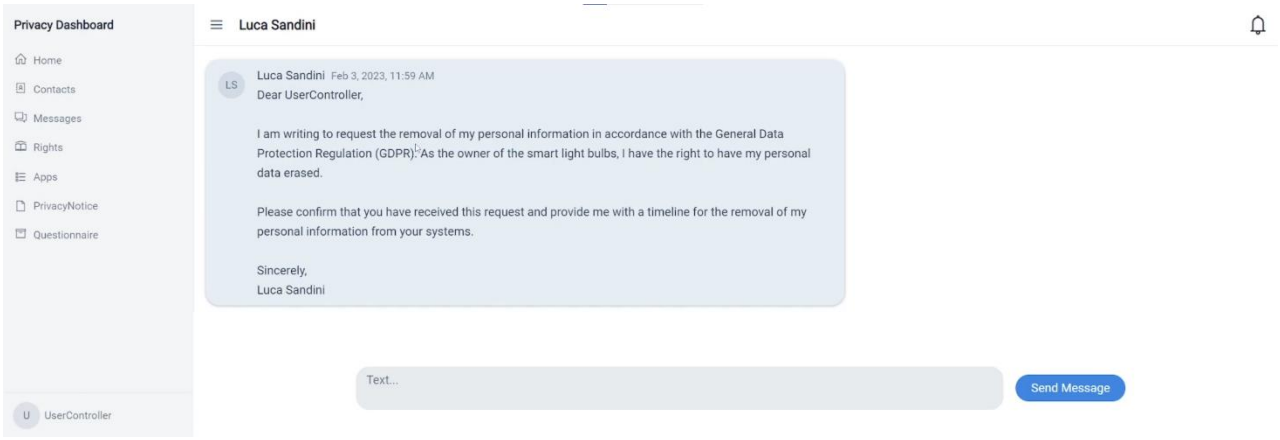
Just as it was the case with the data controller, data subjects are able to access a messaging system that would enable them to communicate directly with their data controllers. This would provide an easy way for data subjects to exercise their rights under the GDPR, such as their right to access their personal data, request its rectification, or object to its processing, relinquishing their consent.

This feature on the dashboard aims to give data subjects a convenient way to manage their personal data and communicate with data controllers. This way of combining an overview of all the relevant contacts and providing a means to quickly message them can be a valuable way to incorporate nudging techniques to enhance compliance with GDPR legislation.

8.5 *The Messages View*



A list of messages received by the data controller in the "messages view"



An example of a conversation taking place between the user (a data controller) and a subject.

The message view provides a quick way for data controllers and data subjects to communicate with each other. The feature includes therefore a chat interface that displays all current and previous conversations that a data subject has had with their data controllers, and vice versa. The message view also includes the ability to search through these previous conversations.

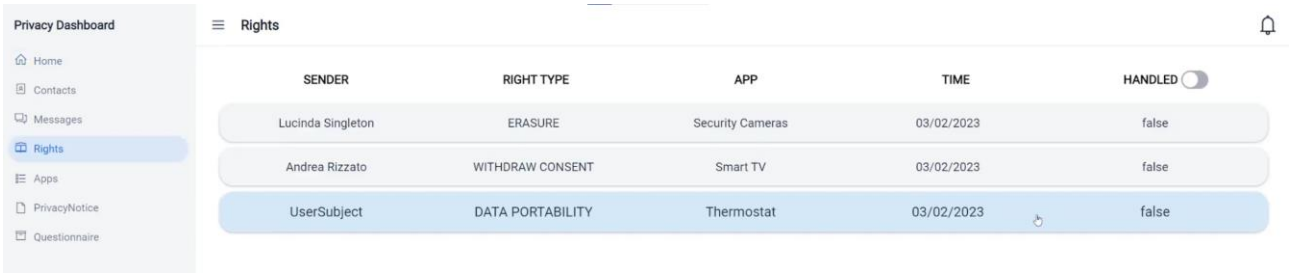
The message view is seamlessly integrated with the contacts list, allowing both data controllers and data subjects to easily initiate a conversation with each other. For instance, when a data subject selects “send message” from the contacts list, they are immediately taken to a message view that shows all previous messages exchanged between them and the selected data controller, as well as allowing to send new messages.

At the moment, the chat interface does not allow for the sending of attachments.

To summarise, the message view on the dashboard provides an easy and efficient way for data controllers and data subjects to communicate with each other. It also helps to ensure that all communication is documented and accessible for reference.

8.6 *The Rights View*

8.6.1 For Data Controllers



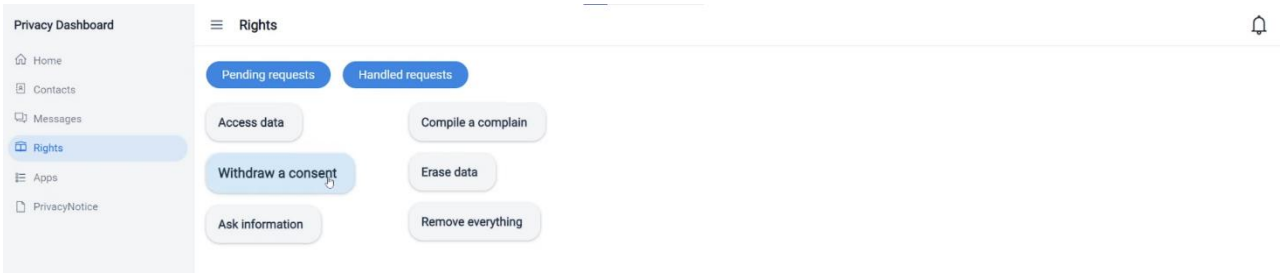
From the perspective of the data controller, a list of all the requests received from different data subjects regarding different applications.

The "Rights" view in the dashboard provides the data controller with a comprehensive overview of all the requests received from data subjects. This view lists all the requests received and provides information such as the type of request, the application it is related to, the date it was received, and the current status of the request. The data controller can quickly see which requests have been handled and which are still pending. Through these features, the dashboard allows the data controller to track how long it is taking to process each request, ensuring compliance with the GDPR's mandated timespans.

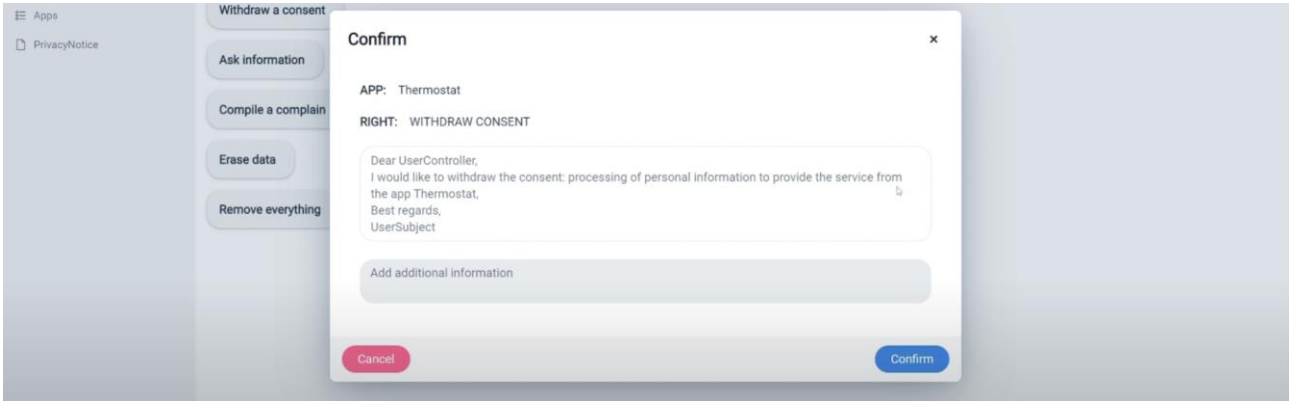
The data controller can also see the details of each request, including the data subject's name and the specific right being exercised.

The "Rights" view therefore aims to provide the data controller with an easy and efficient system for managing data subject requests and ensuring better compliance with the GDPR's rules.

8.6.2 For Data Subjects



The data subject is able, through the "rights" view, to quickly exercise all his GDPR rights.



An example of an automated message generated by the system through which a data subject is telling his data controller they're withdrawing their previously given consent.

The "rights" view on the dashboard is designed to empower **data subjects** and facilitate the exercise of their data protection rights. The main innovation of this feature is that it includes an automatic system for generating messages that can be sent to the data controllers. This system is designed to ensure that data subjects can exercise their rights in a straightforward manner.

The view firstly provides data subjects with several options to choose from. Data subjects can access a pre-formulated message that enables them to request access to their data, withdraw their consent, ask for information about how their data is being used, submit a complaint, or request erasure of their data. The pre-formulated messages are specifically designed to ensure that data subjects can easily exercise their rights.

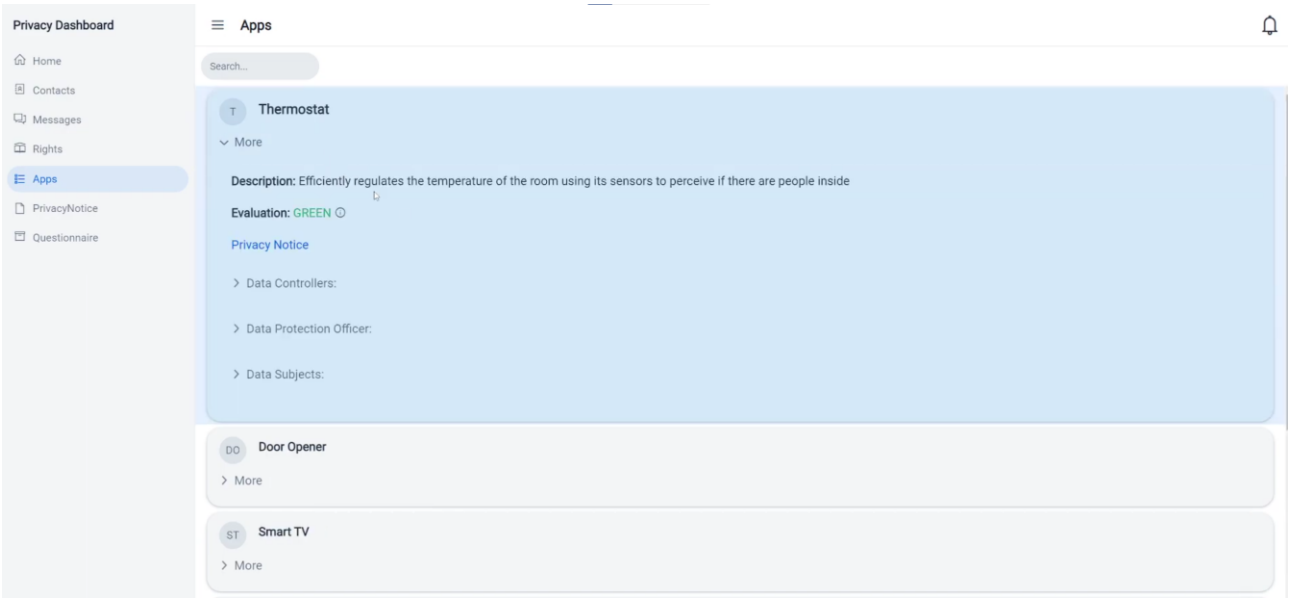
Once the data subject has selected the appropriate message, the system automatically generates its content, also including particulars such as the data controller's contact details. The data subject would then have the option to review and edit the message before sending it to the data controller.

The "rights" view would also allow data subjects to monitor the status of their requests. For example, data subjects could see whether their request has been received, handled, or is still pending. Two menus have been created for this specific need: a "pending requests" one and another named "handled requests".

As in the other views, by aiming to provide a user-friendly interface, pre-formulated messages, and automatic population of relevant information, the system makes it easy for data subjects to exercise the GDPR mandated rights: request access to their data, withdraw their consent, request information, or request erasure.

8.7 *The App View*

8.7.1 For Data Controllers



The "App" view from the perspective of the data controller: a list of all the applications for which he is responsible.

The "App" view of the dashboard is designed to give data controllers a comprehensive overview of all the applications for which they are responsible. The view displays a list of all the applications, and data controllers can click on each application to see a detailed breakdown of information related to that application.

For each application, data controllers can see if there are any joint controllers involved and who they are.

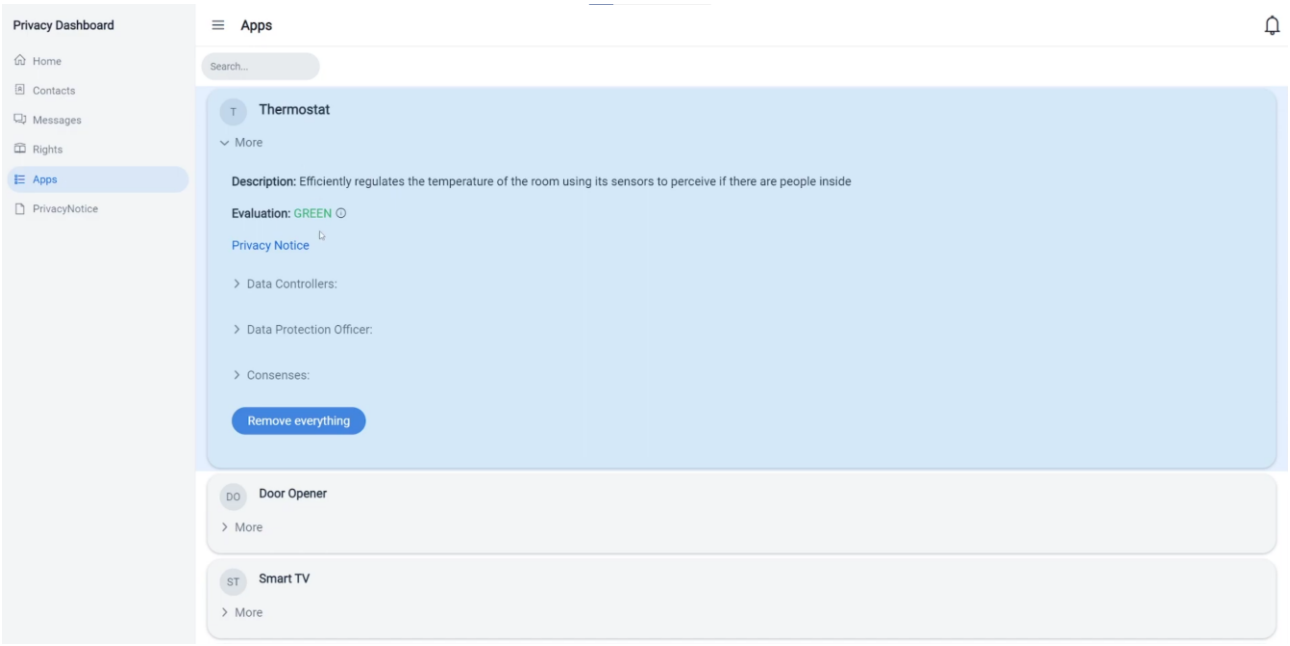
The view also shows the list of all data subjects who are bound to the application, and data controllers can see their personal information and communication history, therefore enabling to quickly see any requests they might have made for access to their data, withdrawal of consent, information, complaints, or data erasure.

Just after its description, every application has also an "Evaluation", ranging from green, to yellow, to red.

This evaluation is based on the "traffic light system", which will be presented in more detail later. For what is important here, when the Data Controller completes a questionnaire and obtains a result, that same result will appear, for the relevant application, in the App view.

Overall, the "App" view of the dashboard provides data controllers with a clear interface to manage all of their applications and the corresponding data subjects, while also being aware of any other data controller (in the case of joint controllership).

8.7.2 For Data Subjects



The data subjects can see a list of all the SIFIS-Home applications which are currently processing their data in this "App" view, together with a number of information about them.

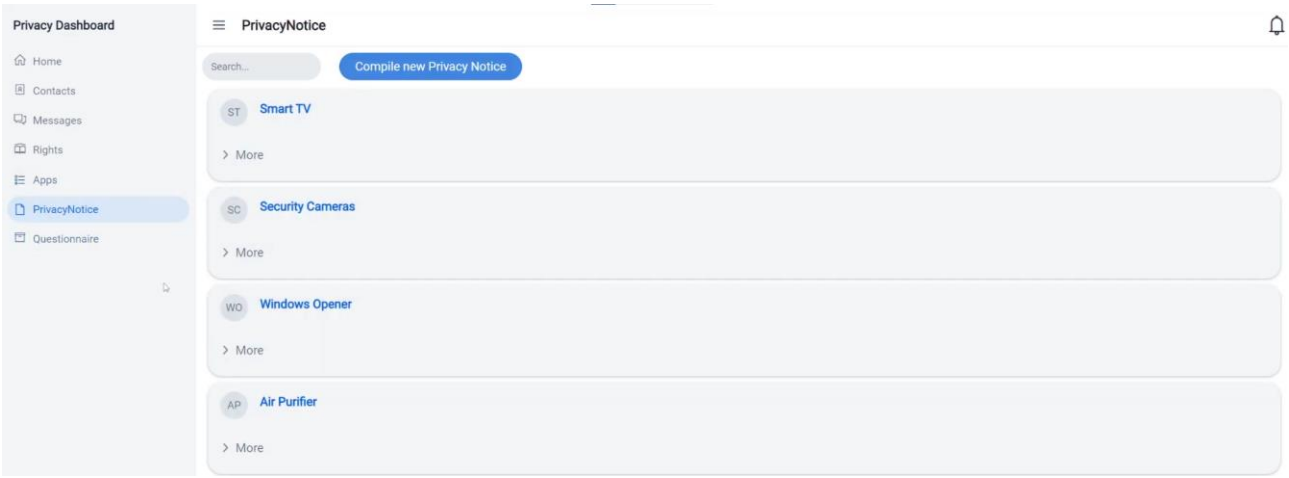
For data subjects, the "app" view allows them to see at a glance all the applications where they have provided their personal data. This view provides a comprehensive list of all the data controllers involved in the processing of their data within each application.

The data subject can view the details of their consent given for each application, including when it was given and for what specific purposes. They can also click on a link to see the specific privacy notices given by each application. These features provide the data subject with transparency over their personal data, allowing them to ensure that their data is only being used in ways that align with their wishes, preferences and given consents.

In addition to viewing the data controllers involved in each application, the data subject can quickly and easily request the removal of all their personal data from a specific app. By simply clicking a button aptly named "remove everything", they can generate an automatic message to be sent to the relevant data controllers, requesting that their data be erased from the application. This not only allows the data subject to exercise their right to erasure, but also streamlines the process for data controllers to fulfill such requests, increasing compliance with data protection regulations.

8.8 *The PrivacyNotice View*

8.8.1 For Data Controllers



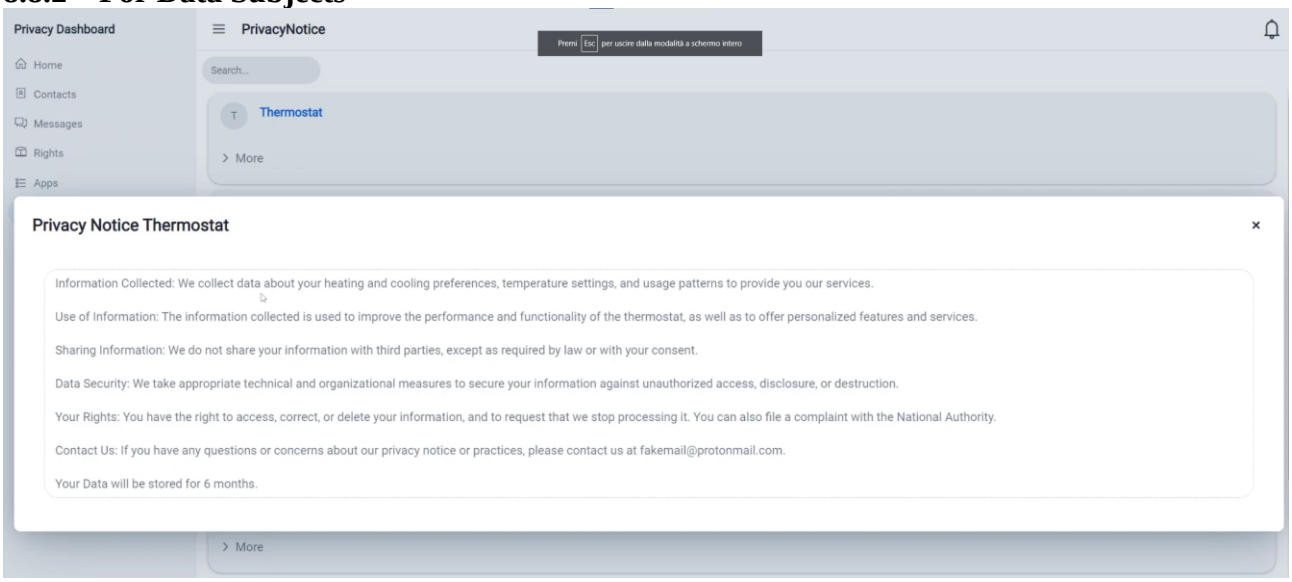
The "PrivacyNotice" view allows data controllers to quickly see all the privacy notices they have provided to their data subject and to quickly edit them or create new ones.

The "PrivacyNotice" view in the dashboard allows data controller to access and manage all the privacy notices associated with the applications for which they are responsible. The view displays a list of applications, along with their associated privacy notices, allowing data controllers to easily navigate and access the information they need.

The view also includes a "Compile New Privacy Notice" button, which opens a text editor where data controllers can create and edit privacy notices for a specific application. The text editor allows data controllers to add, remove, or modify the privacy notice's content as necessary, ensuring that it accurately reflects the application's data collection and current usage practices.

The data controllers may also find the "use template" button very useful, as it allows them to create new privacy notices without having to build them from scratch, provided there are templates available.

8.8.2 For Data Subjects



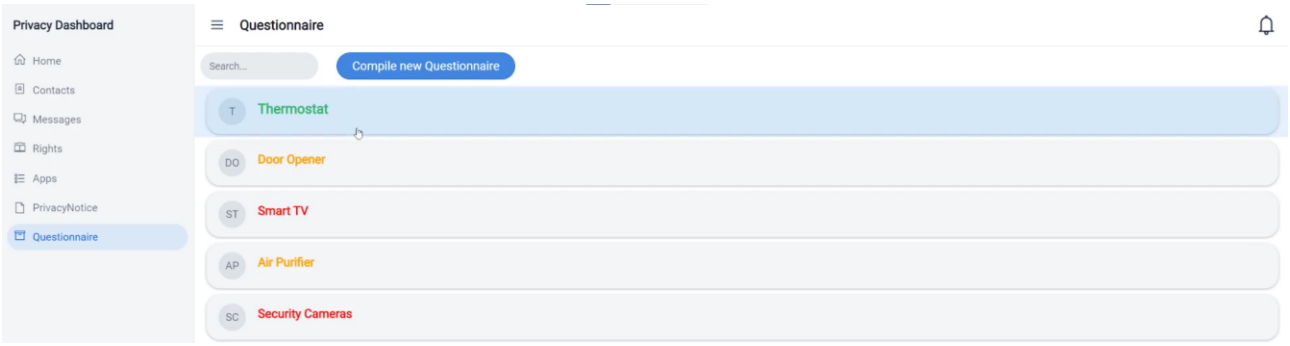
An example of a Privacy Notice viewed from the perspective of the Data Subject in the "PrivacyNotice" view.

From the perspective of a data subject, the "Privacy Notice" view offers the chance to quickly view any of all the privacy notices bound to the SIFIS-Home applications that process their personal data. The

view includes a list of applications, their associated privacy notices, and the data controllers responsible for processing the data.

The view is linked to the previous "App" view, allowing data subjects to quickly navigate to the privacy notice associated with a specific application. Once there, they can review the details of the privacy notice, including the types of personal data collected and how it is used. This information helps data subjects make informed decisions about whether or not to provide their personal data to the application. The "Privacy Notice" view also provides data subjects with an overview of the data controllers responsible for processing their personal data. This includes a single data controller or a multitude of them (in the case of joint controllership).

8.9 *The Questionnaire View for Data Controllers*



A list of all the applications for which the data controller is responsible, which are colour-coded based on the results of their respective questionnaires.

An example of a questionnaire completed by a data controller, whose answers receive different colours based on their effectiveness.

The questionnaire view appears only for data controllers and is designed to evaluate the privacy-friendliness and GDPR compliance of their apps. It uses a traffic light system with red, yellow, and green lights to indicate compliance levels.

First, the data controller is greeted with a view of all the apps that were also shown in the previous “app” view. They are colour-coded based on the evaluation rating they received after answering a questionnaire, which can be performed for every application in the same page.

The questionnaire consists of questions related to GDPR obligations, industry-recognized privacy standards, and software licenses compliance. The questions are designed to elicit information about the software developer's compliance with GDPR and Free and Open-source license obligations.

The Green Light indicates that the software developer has performed a Privacy Impact Assessment based on reasonable assumptions. The software developer has also produced information to comply

with Articles 13, 14, 25, and 32 of GDPR, and the related documents accompany the software. The developer may also have followed the OpenChain specification or other public specifications for licensing compliance, and the software is accompanied by compliance artifacts. The methodology and standards used in creating the privacy impact assessment, compliance artifacts, and other documents should also be publicly available.

The Yellow Light indicates that some of the requirement for obtaining a green light are missing or sub-optimal. In general, a yellow light means that the software developer or data controller can provide all the required information to perform a Privacy Impact Assessment. Information to comply with Articles 13, 14, 25, and 32 of GDPR has been produced and compliance artifacts can be shown. The methodology and standard used in creating the above documents can be made available for compliance assessment, even though it isn't readily visible.

The Red Light indicates that one or more of the conditions outlined in the previous requirements are not satisfied. In this case, the software must be carefully analyzed (potentially on a case-by-case basis) to assess whether it is compliant with GDPR before using it in the EU to process personal data and whether it complies with software licenses obligations.

This questionnaire view, to be used with SIFIS-Home devices, can be very useful for GDPR compliance, especially when considering its potential for legal nudging. It allows data controllers to quickly assess the compliance of their apps with GDPR and Free and Open-source license obligations, and encourages software developers to comply with recognized privacy standards and software licenses compliance specifications, which could increase their chances of being chosen by data controllers for their performance, transparency and safety. Ultimately, this questionnaire view can promote privacy-friendliness and GDPR and software license compliance in the development and deployment of software in real world scenarios, and allows both to protect the privacy and rights of data subjects and to give an easy way for data controllers to be transparent and legally compliant.

8.10 *Future developments*

Further developments will be evaluated later on in the project. Particularly:

- implementation of the dashboard for agents that develop SIFIS-Home technologies;
- implementation of the dashboard for Agents processors;
- implementation of APIs of the privacy dashboard in SIFIS-Home framework in order to allow automatic feeding of data to the dashboard;
- upload of attachments and content storage into the privacy dashboard.

9 Use case legal analysis

The following pilot use cases are implemented in WP6[76]:
1) Turning on/off lights using the control panel;
2) Being notified if someone is at the doorbell;
3) Being alerted if motion sensors detect people presence while the House is in away mode;
4) Being alerted if a software attack is detected;
5) Being alerted if a device is generating anomalous traffic;
6) Policy engine: show that actions are not executed if not allowed;
7) Installation of a third-party application;
8) Creation of different users using the control panel;
9) Face recognition;
10) Parental control;
11) Voice command.

76 These and other use cases are described in D6.1 (Initial pilot use case requirements).

9.1 *Use cases: privacy compliance*

All the applications of pilot use cases are designed to be privacy compliant and to respect the GDPR rules. Intending to provide a privacy analysis, this will start by taking into account all the requirements that are met by each of the applications. Some of them, however, have distinctive traits that will necessitate a more in-depth explanation.

All the data needed for the applications to function in the use cases, and that is processed and sent to the SIFIS-Home cloud, is stored in a CNR server. Therefore, CNR maintains full control of the data. When data is sent so the SIFIS-Home cloud, the data controller is CNR – Consiglio Nazionale delle Ricerche.

We further assume that the house owner does not use the services as a data controller but just in the frame of household activities and therefore the household exception applies to him.

In synthesis, for what concerns GDPR Articles 5 and 6, which state the principles related to the processing of personal data and the lawfulness of processing, these are all respected through the use of a combination of the SIFIS-Home framework, which is privacy-friendly by default and by design, and of the Privacy Dashboard, which will allow the user to not only be made aware of the methodologies and principles behind their processing of data, but also to quickly and easily exercise their rights.

Obtaining a privacy by design and by default environment is nonetheless one of the primary aims of the privacy dashboard and the SIFIS-Home project in general. Therefore, compliance with Article 25 is guaranteed.

The pilot applications also adhere to Articles 9 and 10, which relate to the use of specific kinds of data or data coming from peculiar subjects, such as criminal convicts, as they don't process any of these "special categories" of data.

The *Parental Control* application (use case no. 10) takes into account the presence of a child in a room and aims to signal to the responsible parent if that minor is detected in a different room. This calls into question the need for this specific SIFIS-Home application to take care in being compliant with Article 8, which states that for a minor's data to be processed, caution must be used in ensuring that the holders of parental responsibilities over the child have given their consent. In the specific case of the SIFIS-Home's Pilot Applications, this was considered during testing involving children's data.

For what concerns the rights given to the data subject (Articles 12-23), all of them are easily exercisable through the use of the Dashboard. Specific functionalities in the dashboard which permit the data subject to generate a pre-compiled request, and a "message" view that allows data subjects and data controllers to communicate through a user-friendly interface are the features that guarantee the rights that the data subject wants to exercise.

The dashboard also takes into account the cases where there are more than one data controller (*joint controllerships*), or other subjects such as Data Protection Officers. In this case, all their names and contact addresses are made known to the data subject, who can appeal to each of them for any request or right exertion they may want.
It may be useful to implement a similar system from the perspective of the data controller which would allow him to quickly contact the National Authority to notify personal breaches happening (as per Article 34).

A very similar conclusion can be reached in regard to the Privacy Notice. The information that must be given to the data subject when their data is processed, according to Articles 13 and 14, is easily viewable

in a specific section of the dashboard, for each application. Moreover, a model of a Privacy Notice for every application in this Pilot has been proposed and implemented in the dashboard (see draft privacy notices in annex 2).

The dashboard also allows for a history of processing activities to be maintained and quickly consulted should the need arise. This facilitates compliance with Article 30 (when applicable).

In regard to keeping an adequate level of risk for the data processing taking place according to Article 32, currently the SIFIS Home Pilot applications all run on a proprietary cloud hosted on a CNR machine. Even though the software hub utilized by the applications for their data collection comes from a third party, nonetheless that third party is a partner of the consortium, Sensative. Sensative's platform, Yggio, permits the creation of a database, which however is also located in the SIFIS-Home cloud environment and therefore does not entail any data transfer to third parties.

The control panel within the privacy dashboard allows users to create different user accounts, which are saved to the cloud. Yggio utilizes the KeyCloak application for user management. This application is designed to securely manage user authentication and authorization for cloud-based applications, ensuring that only authorized users have access to personal data and other sensitive information. By using KeyCloak, we can ensure that user information in Yggio's databases (which are always located in the SIFIS-Home cloud, hosted on a CNR machine) is protected and that any data transmitted between the cloud and users is done so in a secure and encrypted manner. This level of security is crucial when it comes to managing personal data and ensuring GDPR compliance, as it helps to prevent unauthorized access or data breaches.

When users download third-party applications, they will be required to log in to DockerHub, which is governed by its own privacy policy[77]. DockerHub is an online repository where developers can share and store their container images, and it is a popular platform used by many software developers and IT professionals.

SIFIS-HOME does not collect any personal data from users during the download process, and therefore cannot be held responsible for the privacy practices of the third-party applications that users download from DockerHub. This is because the third-party applications themselves are developed by independent developers, and they have their own privacy policies and practices that may differ from those of SIFIS-Home.

Users have to review the privacy policy of the application's website or the DockerHub platform where it is hosted. Furthermore, by using DockerHub, users are also bound by its own privacy policy. DockerHub's privacy policy can be found on its website and outlines how the platform collects, uses, and shares users' data.

As many of the features of the applications require snippets of information being recorded, such as the date and time where a certain request happens, care has been taken in ensuring that the data collected is the minimum strictly required for the functioning of the applications, and it is correctly stored in a secure location.

There may be some cases where more personal data is required for the correct operation of the applications. One such case is the Face Recognition app, which allows for the recognition of a certain person through their biometric data. To limit the amount of data sent to the cloud, such an application stores this biometric data locally. The same applies for the Voice Recognition app. No voice or biometric

77 https://www.docker.com/legal/docker-privacy-policy/

information will ever reach the SIFIS-Home cloud, but rather they will all remain stored in the local area network of the user. As a consequence of this, no biometric data are processed by the SaaS provider. When the Face Recognition application is used and it recognizes a certain person, or the Voice Recognition app is activated to give a certain voice command or, again, to be recognized, the only information that reaches the SIFIS-Home servers is a small snippet of text which shows that at a certain hour a certain event happened (in this case, that someone was recognized or that some voice command was used). This approach would allow the application to be compliant with the requirement of data minimization, and offer an example of working and useful features without having to process sensitive data.

While not entirely able to substitute a thorough privacy impact assessment, the Dashboard also offers the chance of answering different questions through the "questionnaire" view that may be of help to determine any critical issues in different applications. This helps in performing the assessments required by Article 35.

9.2 *Use cases: ethical analysis*

The pilot use cases indicated above are evaluated in light of the ethical principles described in paragraph 6.1 (Ethical values):

1. Privacy
2. Physical safety
3. Security
4. Control by the user
5. Discrimination
6. Data commons
7. Free technologies
8. Disadvantaged people
9. Trust.

1) Privacy: all the use cases are implemented in compliance with GDPR and therefore comply with the principles of privacy by design. This provides fair evidence of the fact that the value of privacy is satisfied.

2) Physical safety: some use cases (particularly, No. 1. Turning on/off lights using the control panel and No. 11. Voice command) can interact with devices that could imply physical safety problems; nevertheless, when this happens, physical safety problems are posed by the device more than by the SIFIS-Home application and the nature of the physical safety problem depends on the characteristics and functionalities of the device. It is therefore important to adopt (and possibly alert the user about this via the SIFIS-Home interface) not to use applications that are unsafe. Nevertheless, at the level of the SIFIS-Home application, safety is protected by the security of the application (see below). With these caveats, the value of physical safety is satisfied.

3) Security: security requirements are expressly considered in the design of the application and described in the requirements of the use cases in D6.1 (Initial pilot use case requirements), chapter 5 (Smart home use cases). The value of security is considered in all use cases.

4) Control by the user: The privacy dashboard, implemented with the use cases, gives to the users the possibility to control their personal data. The value of control by the user is satisfied.

5) Discrimination: use cases do not seem to imply algorithms that imply possible discrimination. The value of no discrimination is satisfied.

6) Data commons: use cases are designed to avoid data power concentration; particularly, the SaaS provider is not controller of the personal data, but processor (this implies it cannot use the personal data but for the purpose of providing the services). This enables the design of further SIFIS-Home applications in order to foster the generation of commons out of the aggregated data of different users on a voluntary basis by users or (where applicable) in application of laws. The value of fostering data commons is satisfied.

7) Free technologies: if use case applications will be distributed according to the term of free software licenses, the value of fostering free technologies is satisfied.
8) Disadvantaged people: use case No. 10 (Parental control) allows the protection of minors and therefore satisfies the goal of disadvantaged people protection. The other use cases do not pose a problem of disadvantaged people protection.
9) Trust: in consideration of the above, the value of trust is satisfied.

10 License obligation compliance

The software developed within the SIFIS-Home project[78] is licensed according to the MIT license.
Support for the tool Reuse Software was implemented in SIFIS-Home generate[79]. This enables to follow a fairly good level of automation in the process of choosing a license for the project, adding copyright and licensing information and confirming Reuse Software compliance.

This does not, per se, imply compliance with OpenChain (or other) specification: even if, for example, OpenChain recommends Reuse Software as one component to increase clarity of the licensing and copyright compliance, has higher requirements to achieve full conformance to the specification. But compliance with specification requirements includes organizational measures that, at this stage, cannot be automated.

The partners pay careful attention to reuse libraries and code available according to the terms of non-copyleft licenses compatible with the MIT license and to comply with their legal obligations provided by the licenses of such libraries and code.

78 See https://github.com/sifis-home.
79 See https://github.com/sifis-home/sifis-generate/releases/tag/v0.4.1 release note.

11 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 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 concerning the design of some dashboards that reuse tools already available and add further tools to SIFIS-Home technologies.

During the project, the following actions have been performed:

- A privacy dashboard was implemented as part of the SIFIS-Home technologies (chapter 8);
- Use cases were analyzed to check compliance with GDPR obligations and ethical goals (chapter 9); and
- SIFIS-Home software was licensed under the MIT license and legal compliance was performed adopting the Reuse Software tool (chapter 10).

12 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

2 *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

2 ***Privacy Notices for use cases***

1) Turning on/off lights using the control panel

Such an application allows a logged-in user to control their home lights remotely from outside their house. This is materially done through the use of Yggio, a software hub provided by the partner Sensative, which is deployed on SIFIS-Home cloud on a CNRR device, where, therefore, all data is stored. If the user is inside his house, he can toggle their lights via LAN, without having to pass from SIFIS' servers and therefore without any of their data being processed.

Privacy Policy

Introduction
This Privacy Policy informs about how we collect and process personal information in our home lighting application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:
Login Information: We collect your login information, including your email address and password, in order to allow you to access the App's functionalities remotely.
Usage Information: We collect the date and time of use of the App, as well as login events.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

2) Being notified if someone is at the doorbell

Privacy Policy

Introduction
This Privacy Policy informs about how we collect and process personal information in our home doorbell application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of the App's utilization, such as when the notification of the doorbell being rang happened.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

3) Being alerted if motion sensors detect people presence while the House is in away mode

Privacy Policy

Introduction
This Privacy Policy informs about how we collect and process personal information in our motion detection application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of the App's utilization, such as the date and time of when a presence has been detected while the House is in away mode.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

4) Being alerted if a software attack is detected

Privacy Policy

Introduction
This Privacy Policy informs about how we collect and process personal information in our software attack diagnosis application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information

When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of when the software attack notification has been sent, as well as the reason for which it was sent.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

5) Being alerted if a device is generating anomalous traffic Privacy Policy

Introduction
This Privacy Policy informs about how we collect and process personal information in our anomalous traffic detection application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of the anomalous traffic notification, as well as the reason for which the notification was sent.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

6) Policy engine: show that actions are not executed if not allowed

Introduction
This Privacy Policy informs about how we collect and process personal information in our policy engine application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of the anomalous traffic notification, as well as the reason for which the notification was sent.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security

We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

8) Creating different users using the control panel

Introduction
This Privacy Policy informs about how we collect and process personal information derived from the creation of users in the Control Panel.

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of the anomalous traffic notification, as well as the reason for which the notification was sent.
Login Events.

Usernames and passwords will be encrypted and stored in SIFIS-Home's cloud, hosted on a CNRR machine. The application used to mask and encrypt this kind of data is KeyCloak, specifically made for the safekeeping of databases where usernames are stored.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights

You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

9) Face recognition

Introduction

This Privacy Policy informs about how we collect and process personal information in our home face recognition application (the "App").

Data Controller

The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information

When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of use of the App, as well as login events.

All the biometric data necessary for the application's functionalities are stored locally in your personal devices through your Local Area Network. No biometric data is sent remotely.

Use of Personal Information

We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information

We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention

We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security

We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights

You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

10) Parental control

Introduction

This Privacy Policy informs about how we collect and process personal information in our home minor presence detection application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:
Usage Information: We collect the date and time of use of the App, as well as login events.

All the biometric data necessary for the application's functionalities are stored locally in your personal devices through your Local Area Network. No biometric data is sent remotely.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features. You have the right to lodge a complaint with a supervisory authority.

11) Voice command

Introduction
This Privacy Policy informs about how we collect and process personal information in our home minor presence detection application (the "App").

Data Controller
The data controller responsible for the processing of your personal information is Consiglio Nazionale delle Ricerche (CNR).

Collection of Personal Information
When you use the App, we may collect the following personal information:

Usage Information: We collect the date and time of use of the App, as well as login events.

Vocal data necessary for the application's functionalities is stored locally in your personal devices through your Local Area Network. No such data is sent remotely.

Use of Personal Information
We use your personal information for the following purposes:
To provide you with access to the App's functionalities;
To improve the App's features;
To comply with legal obligations.

Disclosure of Personal Information
We do not disclose your personal information to any third party. All your data is stored on SIFIS-Home systems in CNRR devices.

Data Retention
We will retain your personal information for a period of two months. After this period, your personal information will be securely deleted from our database.

Data Security
We take appropriate technical and organizational measures to protect your personal information against unauthorized or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access.

Your Rights
You have the right to access, rectify, erase, restrict, or object to the processing of your personal information. You also have the right to data portability. To exercise any of these rights, please contact us at [add email]. You can also exercise these rights through the Privacy Dashboard's related features.

You have the right to lodge a complaint with a supervisory authority.