



MOBISTYLE

**MOBISTYLE**

**M**OTivating end-users **B**ehavioral change by combined **I**CT based modular **I**nformation on energy use, indoor environment, health and **l**ife**S**TYLE

**Contract No.:** 723032

**Report:** Modular Information Services for Trust and Privacy

**Work Package:** Work package 5, Task 5.2

**Deliverable:** D5.2

**Status:** Public

---

**Prepared for:**

European Commission

EASME

Project Advisor: Mr Pau Rey-García

**Prepared by:**

HOLONIX

October 05, 2018



*This project has received funding from the European Union's H2020 framework programme for research and innovation under grant agreement no 723032. The sole responsibility for the content lies with the authors. It does not necessarily reflect the opinion of the European Communities. The European Commission is not responsible to any use that may be made of the information contained therein.*



## Content

Executive Summary .....	3
1. Introduction .....	4
2. Increasing trust by making explicit the privacy regulation .....	5
3. Introduction to the General Data Protection Regulation (GDPR).....	6
4. Key Security Objectives of GDPR.....	9
- Personal data .....	9
5. Core Actors of the GDPR .....	12
6. Key Requirements of GDPR and Data Security .....	15
- Assessing Security Risks .....	15
- Preventing Attacks.....	16
- Monitoring to Detect Breaches .....	17
- Quality of Protection.....	17
7. Actions for Personal Data Management.....	19
8. MOBISTYLE-related considerations .....	25
9. A GDPR-related mapping within MOBISTYLE.....	27
10. The action plan timeline and concluding remarks.....	28
11. References .....	29
Annex 1.....	30

## Executive Summary

The main aim of this document emerges from the need to clarify the definitions and procedures related to the application of the General Data Protection Regulation (GDPR) to the MOBISTYLE system. Since May 2018, when the new GDPR became legally obliging, several regulatory changes have been introduced on the European level. The GDPR poses explicit requirements for personal data collection and processing that require engagement of all the partners within the MOBISTYLE consortium, which is distributed across five EU countries (Netherlands, Denmark, Slovenia, Poland, and Italy).

This document introduces the main definitions of GDPR and a plan of activities to address trust and privacy within the MOBISTYLE project. The GDPR-specific requirements should address personal data collection and management at different EU demonstration sites as well as in distributed modules of the ICT systems that is still under development. Therefore, content of this report aims at informing the consortium partners about the key concepts and purpose of GDPR that may impact their own activities in respect to the personal data collection, data processing, software development, as well as re-definition of technical specifications within the project. For that purpose, the document elaborates specific steps necessary to undertake in order to address the GDPR requirements in terms of contractual and technical responsibilities. Finally, the document provides an action plan specifying further steps necessary to take in order to face the personal information management.

## 1. Introduction

This report constitutes the first and initial part of a four-phases procedure defined to address trust and privacy within the MOBISTYLE project. Starting from the definition of GDPR requirements, the document outlines the key concepts of GDPR and provides specific directions, i.e. an action plan, that will be taken in order to address and assess impact of GDPR on the MOBISTYLE project. It distinguishes contractual and technical aspects that will be used to define data controllers, processors, personal data types, data flows, and data transformation protocols on diverse levels of detail.

The second phase of the procedure will involve all the project partners and a legal expert in order to increase awareness on the privacy and GDPR issues and to identify responsibilities of each partner involved in personal data collection and data processing. The necessary implementation measures will be identified in agreement with the MOBISTYLE partners during the second phase scheduled for October 2018 (month 24). The second phase activities will result in a report that will be shared with the consortium during November 2018 (month 26). The report will also be published in the deliverable D5.6 during the final phase of the project (month 39-42).

The third phase of the procedure (month 26 - month 32) is dedicated to the implementation of steps that will be specified during the second phase, when all the relevant parties will have to adopt and implement specific actions according to their roles and responsibilities assigned during the second phase.

The fourth and final phase (month 32 – month 39) will consist of a GDPR assessment and validation procedure demonstrating to what extent the project partners have managed to address the issues related to GDPR within the project. Deliverable D5.6 will report the results of the implementation and validation procedure.

## 2. Increasing trust by making explicit the privacy regulation

Transparency on how personal data is used aims at increasing the trust of consumers as well as providers of services. Privacy policies, transparent and obligatory, are now becoming more human-centered with the explicit requirements of GDPR. Easily accessible and unambiguous, privacy policy specifications should provide users with a better understanding of what they are letting organizations do with their personal data. Users of services do not need to read any more long documents written in bureaucratic terminology of lawyers. Information provided to the users that declares in a clear and simple language what are rights of users and how their data is treated should be written in a comprehensive and unambiguous manner in order to address actual users of digital services. A result of such increase of transparency and control that personal data can be accessed, revised, and/or removed, without ending up in the wrong hands, user's trust should increase<sup>1</sup>. Having respected user's requirements and needs, their willingness to share personal information is expected to increase.

On the other hand, organizations providing services that require collection and use of personal data, by respecting GDPR requirements, may increase transparency and build trust of users. The increase of transparency requires that organizations that are collecting and processing personal data clarify how they use and process the data by means of clearly presented consents and privacy statements.

A privacy policy, besides providing a statement, requires elaboration of all the necessary requirements, discovery and management of personal data as well as capacity to define and implement protection measures, request-responses, and reporting mechanisms that should accomplish promises and expectations of users who give their consent to provide an organization with their personal information. GDPR specifically provides guidelines and legally obliging requirements in order to enhance trust by assuring a fair and secure treatment of personal data.

---

<sup>1</sup> Users' survey: <https://www.realwire.com/releases/Half-of-UK-consumers-dont-believe-organisations-care-about-their-privacy>  
H2020 MOBISTYLE\_723032\_WP5\_D5.2



### 3. Introduction to the General Data Protection Regulation (GDPR)

The intention of GDPR [1] is to “contribute to the accomplishment of an area of freedom, security, and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons” (Paragraph 2) as well as to “harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.” (Paragraph 3)

The GDPR is the new regulation on data protection for personal data across the EU. It replaces the earlier 1995 EU Directive on data protection [2]. The key takeaways of GDPR can be summarised as follows [2]:

- The new data protection regulation from the EU, with an implementation date of May 25, 2018. Organizations anywhere in the world that collect or process personal data on EU residents must comply with this regulation.
- Complying with the GDPR requires both organizational and technological measures in response. Organisational measures *in some cases include*: appointing a Data Protection Officer (see Section 5, p. 13), policies and training on handling personal and sensitive personal data (Sections 7, 10), and an approach for executing a Data Protection Impact Assessment (DPIA). Technological measures include data classification, data loss prevention, encryption, managing consent more explicitly, data transfer limitations, and technologies that enable data subjects to exercise their rights to access, rectify, and erase personal.
- The GDPR is focused on the protection of personal data, not only the privacy of personal data.
- All organisations are required to take action to develop a coordinated organizational and technological response to address the new requirements.

The GDPR is important for two key reasons:

- It applies to organisations anywhere in the world that controls or processes personal data on EU residents.
- The cost of non-compliance is significant, with a financial penalty of up to a €20 million fine or 4% of total worldwide annual turnover of the preceding financial year.

## What the new EU GDPR means in 1 minute


The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

**Tough penalties:** fines of up to


**4%** of annual global revenue

or


**€20 million**, whichever is **greater**.





The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.





The **definition of personal data** is now broader and includes identifiers such as

  
genetic


  
mental

  
cultural


  
economic


  
social identity.

**Obtaining consent** for processing personal data must be clear, and must seek an affirmative response.

 **Yes**

Parental consent is required for the processing of **personal data of children** under age 16.



 Data subjects have the **right to be forgotten** and erased from records.

Users may request a copy of personal **data in a portable format**.

Figure 1: A brief introduction to the basic elements of GDPR.



Although the protection of personal data is not absolute, it should be considered and balanced proportionally with other fundamental rights such as respect for private and family life, home and communications, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity (Paragraph 3). It further describes that given technological development, globalization, and collection and sharing of personal data that “a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.” (Paragraph 7)

GDPR applies to the personal data controllers and data processors who are based in the EU as well as to the companies that are not based in the EU but who offer services or monitor behaviour of the EU residents from outside the EU borders.

One of the main goals of GDPR is to increase trust and privacy between users and providers of services. A legal duty to keep records of personal data processing activities, according to GDPR, have only those entities for which processing of personal data is a regular activity or poses a threat to individuals’ rights and freedoms, or concerns sensitive data or criminal records.

The data encryption is only one of the components of a broad security strategy considered in GDPR. It obliges organizations to implement assessment, preventive, and inspection controls in respect to the sensitivity of the personal data they deal with.

The EU increases enforcement powers in order to ensure compliance with the GDPR by enforcing huge fines of up to 4% of the global annual revenue upon non-compliance.

In order to understand if and how this legal obligation applies to the MOBISTYLE project an in-depth analysis with the legal experts is required. Identification of personal data and evaluation of data that fall within the scope of GDPR also requires active and informed involvement of MOBISTYLE partners who deal with data and, perhaps, sensitive personal data. This section explains the key concepts that should be considered in order to define if and how data collected from end-users within the MOBISTYLE distributed information system should be treated in order to assure information transparency, trust, and privacy.



#### 4. Key Security Objectives of GDPR

The four main steps towards assuring compliance with GDPR include four phases with the aim to discover, manage, protect, and report all the relevant issues in respect to personal data.



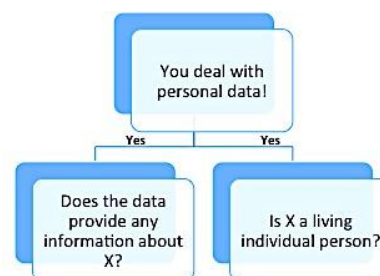
Figure 2: The four-step procedure towards accomplishment of the GDPR compliance.

The initial step towards the GDPR compliance requires assessing whether the GDPR applies to an organization, i.e. a MOBISTYLE partner. In case GDPR applies to an organization, i.e. the consortium partner, there should be identified what data that the organization controls fall under the scope of GDPR. This analysis includes understanding what data is collected and where it resides. Such an analysis might require professional auditing lead by legal experts.

##### - Personal data

Personal data is defined as any information that relates to an actual living individual (not legal entities or deceased persons).

In addition, personal data provides information that might be used to identify a person, also referred to as 'natural person' and 'data subject' (see Art. 4, definition 1).



##### Art. 4, Definitions, Paragraph 1

**'personal data' means any information relating to an identified or identifiable natural person ('data subject');** an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal information, from a legal point of view, can be characterized as:

- Personal data
- Sensitive personal data

Personal data includes information such as name, surname, home address, e-mail address or location data acquired from the map on a mobile phone. This kind of personal data is most commonly collected from employees, clients, i.e. users of services, or from external suppliers of services.

## Discover

In order to identify if data collected by an institution or a company, are personal data, an analysis should be performed to *Discover* to which category collected data belong.

According to specific field of application, personal data can be additionally clustered in several groups, i.e. personal information types: financial data (bank account, IBAN), demographic data (name, gender,



date of birth, age, nationality), contact channels (phone number, address, email), government identifiers (passport number, ID number, social security, driver license), digital identifiers (IP address, coordinate), social media (Twitter, FB, LinkedIn), and sensitive personal information (health, sexual orientation, political views, religious affiliations, genetic, ethnicity, etc.).

GDPR refers to sensitive personal data as “special categories of personal data” (Article 9). Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (Article 10).<sup>2</sup>

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible. Therefore, data forms used to collect user’s Informed Consent at the MOBISTYLE demonstration sites might also fall within the scope of GDPR.

Pseudonymised personal data may also fall within the scope of the GDPR if the pseudonym might be easily associated with a particular individual.

The key principles that should be followed when personal data is collected concern the need to define a precise scope of data use and minimum information requirements. In other words, personal data should be collected with a clearly defined purpose, and should not be used for anything else beyond the defined purpose.

Individuals to whom data relates are from a legal point of view characterized as **data subjects** who should be informed about the purpose for which their data is collected and used. The types of personal data collected from data subjects should be explicitly declared and presented to them at the moment of data collection as well as at any other moment, upon an individual request of the data subject whose data is getting collected and processed. The agreement to provide personal data is regulated via consent.

Personal data processing is based on **an explicit consent**. The purpose of the strict GDPR rules is to ensure that the individual understands what he/she is consenting to. **The consent** should be freely given, specific, informed and unambiguous. A request to collect data should be presented in clear and plain language. The consent should be given by an **affirmative act** and not passively. For that purpose, a check box in a web service or signing a form can be used.



#### Art. 4, Definitions, Paragraph 11

"consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

<sup>2</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

Regarding the age of individuals who can give consent, GDPR should be aligned with national law. Parental consent is required for processing of personal data pertaining to children. The age threshold, in case of children, varies between 13 and 16 amongst different countries. In order to align the consent request procedure across countries where demonstration cases take place, MOBISTYLE consent form provided to users could adopt the upper age limit of 16.

Adopting a classification scheme that applies throughout the MOBISTYLE distributed system could facilitate discovery of personal data, as well as, potential responses to data subject requests to review their personal data, to revise them, to retrieve them or to send them to a third party. A data classification schema can allow to identify and to process such personal data requests much faster.

**Discovery phase includes:**

- Search and identification of personal data (Article 15 (3))
- Facilitation of data classification (Articles 30 (2)(b-d); 32 (2))
- Maintenance of an inventory of personal data holdings (Article 30 (1-3))

Some commercial services provide possibility to easily search and identify personal data. For instance, Microsoft Azure helps facilitate data classification with Azure Information Protection labels and data source annotation in Azure Data Catalog.

A distributed and open characterization of MOBISTYLE services employs also a proprietary platform of Microsoft, the Azure Cloud. The Cloud database has been just recently introduced in the MOBISTYLE ICT platform and constitutes only a component of the whole MOBISTYLE Platform. Therefore, its employment in data management is limited due to the distributed nature of the platform. Some personal data collected from the MOBISTYLE users are also stored, and partially processed in other databases (local databases of the demo-site holders) located in Italy, Denmark, Netherlands, Poland, and Slovenia. Therefore, an alternative and, perhaps, an open source solution<sup>3</sup> fitting to the demands of the Open Platform that is currently in its development phase, could be incorporated as to index, search, and maintain inventory of personal data across the distributed modules. This activity will be addressed in the second and third phase of GDPR action plan of MOBISTYLE.

The following section (Section 5) defines the core GDPR actors whose roles and responsibilities are crucial for the implementation and execution of procedures related to personal data. It outlines how data subjects may interact with other GDPR-related actors from a contractual perspective in order to fulfil the main data security requirements (Sections 6) and recommended actions (Section 7) for personal data treatment and safeguarding along the *Manage*, *Protect* and *Report* phases.

---

<sup>3</sup> See e.g. ODRL model <https://www.w3.org/TR/odrl-vocab/>  
H2020 MOBISTYLE\_723032\_WP5\_D5.2

## 5. Core Actors of the GDPR

The core actors who should be considered in the analysis and implementation of GDPR are defined as:

- Data subject
- Data controller
- Data processor

**Data Subject** is defined as a person who can be identified directly or indirectly by means of an identifier. For example, an identifier can be a national identifier, a credit card number, a username, or a web cookie.

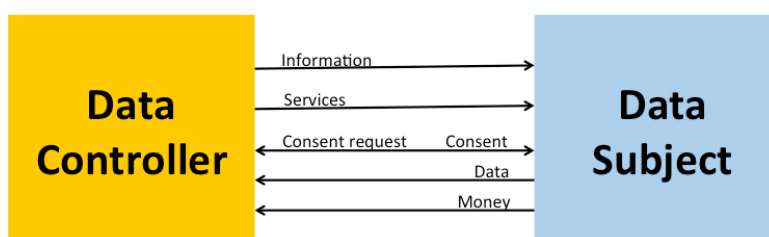


Figure 3: The key relationships between Data Controller and Data Subject.

Figure 3 depicts the key relationships between a data controller and a data subject. Data controller (simply, Controller) provides data subjects (simply, Subject) with the relevant information and services. Controller is defined (Paragraph 7) as a natural or legal person who determines the purpose and means of personal data processing. In order to enable functioning of the services, Subject provides the Controller with the relevant data. In contractual terms, GDPR imposes the need for an explicit agreement between the data controller and subject in terms of consent that has been outlined in section 3. Controller should explicate, informing Subject, what kind of data is relevant for functioning of the services. In the case of commercial services data Subject provides the Controller with money and/or payment details. Commercial relationships and interactions between the MOBISTYLE data controllers and data subjects is currently out of scope, but might be relevant for possible future exploitation of the platform.

### Art. 4, Definitions, Paragraph 7

**'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;

**Processor** is defined (Paragraph 8) as a natural or legal person who is appointed by Controller to processes personal data.

**Art. 4, Definitions, Paragraph 8**

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

**Recipient** is defined as natural or legal person, agency or any other body to whom the personal data is disclosed. For example, a researcher analyzing sensitive personal data from wearable devices within the MOBISTYLE project fall under the category of Recipient. Also, a database administrator who manages user accounts or structured data from the user Consent forms is a Recipient.

**Third party** is defined as any natural or legal person, agency or any other body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorized to process the data. For example, in the MOBISTYLE consortium, partners or subcontractors who would have access to personal data of end-users would belong to this category.

**Supervisory Authority** is defined as an independent public authority established by a Member State (known as the National Data Protection Authority under the current EU Data Protection Directive), or auditing agency. In the case of MOBISTYLE, Supervisory Authorities of several EU countries might be relevant in case of potential issues related to security of personal data.

**Data Protection Officer** is defined as an individual working for a Controller or a Processor with extensive knowledge of the data privacy laws and standards. The Data Protection Officer (DPO) should advice the controller or the processor of their obligations according to the GDPR and should monitor its implementation. The DPO acts as a liaison between the controller/processor and the supervisory authority. A DPO for example can be a Chief Security Officer (CSO) or a Security Administrator.

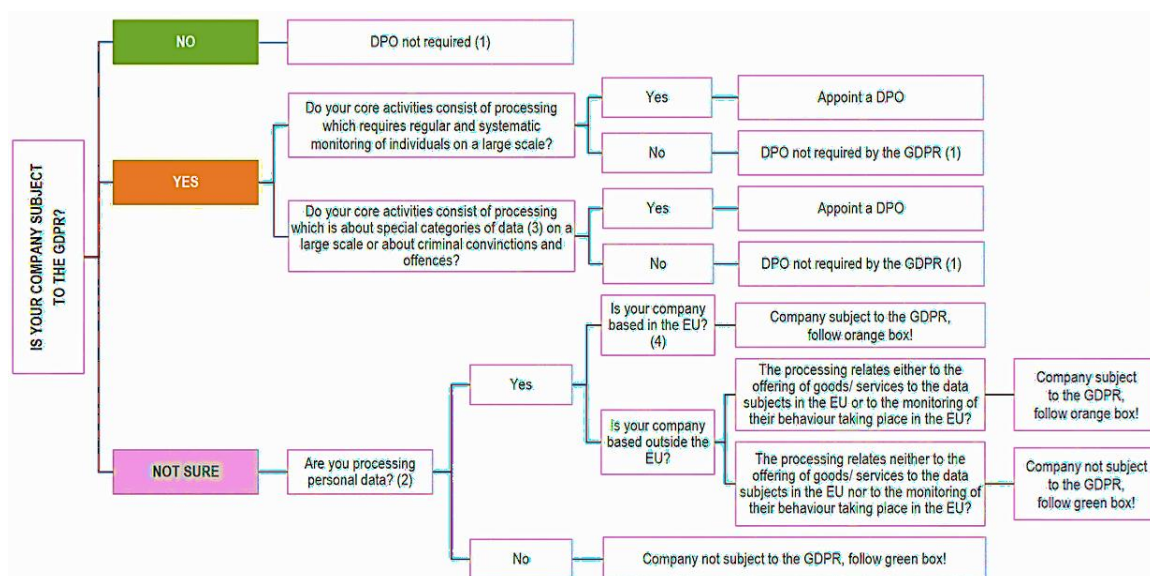


Figure 4: A decision tree helping to clarify if a Data Protection Officer should be appointed in an organization.



Figure 4 provides an insight into information that a company needs to consider as to decide necessity of appointing a DPO.

The following sections outline the main data security requirements of GDPR (Sections 6) and recommended actions (Section 7) for personal data treatment and safeguarding along the *Manage*, *Protect* and *Report* phases.

## 6. Key Requirements of GDPR and Data Security

Personal data security, according to GDPR is related to data inventory specification and records processing, risk awareness, and response to modifications necessary to address rights of data Subject.

### List of GDPR requirements addressing personal data security:

#### - Data inventory

- Records of processing, (Article 30)

#### - Risk awareness

- Data protection impact assessment, (Article 35)

#### - Application modification

- Right of access by the data subject, (Article 15)
- Right to rectification, (Article 16)
- Right to erasure ('right to be forgotten'), (Article 17)
- Right to restriction of processing, (Article 18)
- Notification obligation regarding rectification or erasure of personal data or restriction of processing, (Article 19)
- Right to data portability, (Article 20)

#### - Architecture integration

- Security of processing, (Article 32)
- Principles relating to processing of personal data, (Article 5)
- Responsibility of the controller, (Article 24)
- Data protection by design and by default, (Article 25)
- Processor, (Article 28)
- Communication of a personal data breach to the data subject, (Article 34)

The reminder of this section introduces some guidelines that, mostly, data controllers and processors should consider while dealing with personal data. This includes various preventing measures and risk assessment that is required before any personal data is processed.

#### - Assessing Security Risks

**Data Protection Impact Assessment (DPIA)** is obligatory only if a proposed data processing activity involves a high risk to the rights and freedoms of individuals. DPIA is a procedure that aims at describing data treatment and assessing the necessity and proportionality of the adopted data treatment. This procedure should help to manage risks for the rights and freedoms of individuals deriving from the processing of personal data. It includes evaluation of risks and specification of the measures for mitigation of the risks.

#### Art. 35

The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks

DPIA is an instrument relevant to the principle of "accountability" as it assists the data owner not only to comply with the requirements of the GDPR, but also to demonstrate that it has taken appropriate measures to ensure compliance (see Article 24).

In the cases when the data processing operation is dynamic and subject to ongoing changes, the DPIA is a continuous process.

#### - Preventing Attacks

Importance of implementing preventive measures is stressed by GDPR, including specific recommendation of several standard techniques that are listed below.

#### Preventive measures:

- Encryption (Article 32)
- Anonymization and Pseudonymization (Article 28)
- Privileged User Access Control
- Fine-grained Access Control
- Data Minimization

GDPR considers encryption as one of the core techniques to assure that the personal data are unintelligible to any person who is not authorized to access them. Accordingly, even in the cases of a data breach, Controller does not need to notify data subjects if data is encrypted and so unintelligible to any person accessing it (Article 34). Thus, encryption significantly reduces burden related to possible data-breach notification procedures.

Data anonymization is the technique of completely scrambling and masking the data. In this way, pseudonymization reduces the linkability of a data set with the original identity of a data subject. GDPR recognises that anonymization and pseudonymization are convenient techniques that can reduce the risk of both accidental and intentional data disclosure.

#### Art. 26

**The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.**

In addition, GDPR requires a controlled and restricted behavior of privileged users who have access to personal data in order to prevent possible attacks from insiders and compromised user accounts. therefore, Article 29 states that Processor and any person who has access to personal data, should not process those data except on instructions from the Controller.

A fine-grained access control methodology is another measure recommended by GDPR as to ensure that personal data is accessed selectively and only for a defined purpose. This kind of fine-grained access control can help organizations to minimize unauthorized access to personal data. So, Article 25



states that only personal data that are necessary, for each specific purpose of the processing, are processed.

Finally, a very adequate prevent measure that GDPR recommends relates to minimisation of the personal data collection and retention of personal data as much as possible. The amount of information that is collected and processed should be reduced only to the aim that necessities a specific activity. Thus, collected and processed personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') (Article 5).

#### - **Monitoring to Detect Breaches**

Even if preventive security measures addressed above minimise the risk of attacks and data disclosure, they cannot eliminate completely the possibility of personal data breach. Therefore, GDPR incorporates recommendations for monitoring and alerting of possible data breaches.

#### **Monitoring activities:**

- Audit data
- Monitor and timely alert

GDPR requires from Controllers to keep recording or auditing of the activities on personal data. Moreover, Article 33 of GDPR recommends that these records must be maintained centrally under the responsibility of Controller. The aim of this measure is to twofold: it prevents possible attempts of processors and third-parties to modify or destroy the audit records; auditing may provide important information that could be requested in possible forensic analysis related to data breach.

#### - **Quality of Protection**

Security of ICT systems has been always playing an important, and, perhaps, a central role. GDPR additionally stresses the security management as a mandatory requirement. In order to increase the quality of protection GDPR provides certain guidelines that can facilitate the security controls.

#### **The key security principles:**

- Data Security by design and by default
- Centralization
- Comprehensive Security

The GDPR positions data protection as a central component of any ICT system as the data security should be assured by default and by design. Incorporating security principles during the initial phases of an ICT system design should increase the security and ensures that technical security controls may perform as expected. As stated in Article 25, "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".



Implementing a centralized administration is another security principle of GDPR. In particular, distributed and modular systems that are dealing with security of multiple applications and sub-systems may have advantage of a centralized administration as it can help to take immediate actions in case of a breach. Other advantages of centralized controls are related to uniformity of data controls and management of distributed information processing requests across the system components.

Comprehensive Security principle requires a readiness to threats and attacks that can come from diverse and multiple sources. Thus, in order to assure quality of data protection, an organization should be ready to face possible attacks from any direction. This requirement is aligned with GDPR request to assure protection of personal data along all stages of the data lifecycle.

## 7. Actions for Personal Data Management

Privacy policy compliance and personal data management is a continuous activity. Specific steps and activities related to the personal data management are outlined in the action list below. Those actions that are associated with mandatory requirements of GDPR refer to the corresponding GDPR articles. Non-mandatory actions intend to facilitate execution of GDPR-compliance in a sustainable manner over time.

### A recommended action list for management of personal data<sup>4</sup>:

#### 1. Maintain Governance Structure

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, Privacy Counsel, CPO, Representative), (mandatory for article 27)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer/Official (DPO) in an independent oversight role (mandatory for articles 37, 38)
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. Job descriptions), (mandatory for article 39)
- Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy, (mandatory for article 38)
- Engage stakeholders throughout the organization on data privacy matters (e.g., information security, marketing, etc.)
- Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to external stakeholders on the status of privacy management (e.g., regulators, third-parties, clients)
- Conduct an Enterprise Privacy Risk Assessment (mandatory for articles 24, 39)
- Integrate data privacy into business risk assessments/reporting
- Maintain a privacy strategy
- Maintain a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies

#### 2. Maintain Personal Data Inventory

- Maintain an inventory of personal data holdings (what personal data is held and where) , (mandatory for article 30)
- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)

---

<sup>4</sup> The action list adapted from the Nymity framework <https://info.nymity.com/gdpr-compliance-toolkit>  
H2020 MOBISTYLE\_723032\_WP5\_D5.2



- Maintain flow charts for data flows (e.g. between systems, between processes, between countries)
- Maintain records of the transfer mechanism used for cross-border data flows (e.g., standard contractual clauses, binding corporate rules, approvals from regulators), (mandatory for articles 45, 46, 49)
- Use Binding Corporate Rules as a data transfer mechanism, (mandatory for articles 46, 47)
- Use contracts as a data transfer mechanism (e.g., Standard Contractual Clauses) , (mandatory for article 46)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use regulator approval as a data transfer mechanism, (mandatory for article 46)
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism, (mandatory for article 45, 48, 49)
- Use a privacy shield (e.g. EU-US Privacy Shield) as a data transfer mechanism, (mandatory for article 46)

### 3. Maintain Data Privacy Policy

- Maintain a data privacy policy, (mandatory for articles 5, 24, 91)
- Maintain an employee data privacy policy
- Document legal basis for processing personal data, (mandatory for articles 6, 9, 10)
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)
- Maintain an organizational code of conduct that includes privacy

### 4. Embed Data Privacy Into Operations

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data) , (mandatory for articles 9, 10)
- Maintain policies/procedures for collection and use of children and minors' personal data, (mandatory for articles 8, 12)
- Maintain policies/procedures for maintaining data quality, (mandatory for articles 5)
- Maintain policies/procedures for the de-identification of personal data, (mandatory for article 89)
- Maintain policies/procedures to review processing conducted wholly or partially by automated means, (mandatory for articles 12, 22)
- Maintain policies/procedures for secondary uses of personal data, (mandatory for articles 6, 13, 14)
- Maintain policies/procedures for obtaining valid consent, (mandatory for articles 6, 7, 8)
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices, (mandatory for article 5)
- Integrate data privacy into direct marketing practices, (mandatory for article 21)
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices

- Integrate data privacy into digital marketing practices (e.g., mobile, social media, behavioural advertising)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media practices, (mandatory for article 8)
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into delegate access to employees' company e-mail accounts (e.g. vacation, LOA, termination)
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into research practices, (mandatory for articles 21, 89)

## 5. Maintain Training and Awareness Program

- Conduct privacy training, (mandatory for article 39)
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training, such as HR, security, call center
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information, e.g., an internal data privacy intranet
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g., an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. numbers of participants, scoring)
  
- Enforce the Requirement to Complete Privacy Training
- Provide ongoing education and training for the Privacy Office and/or DPOs (e.g. conferences, webinars, guest speakers)
- Maintain certification for individuals responsible for data privacy, including continuing professional education

## 6. Manage Information Security Risk

- Integrate data privacy risk into security risk assessments, (mandatory for article 32)
- Integrate data privacy into an information security policy, (mandatory for articles 5,32)
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring) , (mandatory for article 32)

- Maintain measures to encrypt personal data, (mandatory for article 32)
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties) , (mandatory for article 32)
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Maintain backup and business continuity plans
- Maintain a data-loss prevention strategy
- Conduct regular testing of data security posture, (mandatory for article 32)
- Maintain a security certification (e.g., ISO)

## 7. Manage Third-Party Risk

- Maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates), (mandatory for articles 28, 32)
- Maintain procedures to execute contracts or agreements with all processors, (mandatory for articles 28, 29)
- Conduct due diligence around the data privacy and security posture of potential vendors/processors, (mandatory for article 28)
- Conduct due diligence on third party data sources
- Maintain a vendor data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct ongoing due diligence around the data privacy and security posture of vendors/processors
- Review long-term contracts for new or evolving data privacy risks

## 8. Maintain Notices

- Maintain a data privacy notice that details the organization's personal data handling practices, (mandatory for articles 8, 13, 14)
- Provide data privacy notice at all points where personal data is collected, (mandatory for articles 13, 14, 21)
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark to increase customer trust

## 9. Respond to Requests and Complaints from Individuals

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data, (mandatory for article 15)
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data, (mandatory for article 16, 19)
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing, (mandatory for articles 7, 18, 21)
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for data portability, (mandatory for article 20)
- Maintain procedures to respond to requests to be forgotten or for erasure of data, (mandatory for articles 17, 19)
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data protection complaints
- Monitor and report metrics for data privacy complaints (e.g. number, root cause)

## 10. Monitor for New Operational Practices

- Integrate Privacy by Design into system and product development, (mandatory for article 25)
- Maintain PIA/DPIA guidelines and templates, (mandatory for article 35)
- Conduct PIAs/DPIAs for new programs, systems, processes, (mandatory for articles 5, 6, 25, 35)
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes, (mandatory for articles 5, 6, 25, 35)
- Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process, (mandatory for article 35)
- Track and address data protection issues identified during PIAs/DPIAs, (mandatory for articles 35)
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate), (mandatory for article 36)

## 11. Maintain Data Privacy Breach Management Program

- Maintain a data privacy incident/breach response plan, (mandatory for articles 33, 34)
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol, (mandatory for articles 12, 33, 34)
- Maintain a log to track data privacy incidents/breaches, (mandatory for article 33)
- Monitor and Report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider

- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

## **12. Monitor Data Handling Practices**

- Conduct self-assessments of privacy management, (mandatory for articles 24, 39)
- Conduct Internal Audits of the privacy program (i.e., operational audit of the Privacy Office)
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third-party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability, (mandatory for articles 5, 24)
- Maintain certifications, accreditations, or data protection seals for demonstrating compliance to regulators

## **13. Track External Criteria**

- Identify ongoing privacy compliance requirements, e.g., law, case law, codes, (mandatory for article 39)
- Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry associations, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes
- Identify and manage conflicts in law



## 8. MOBISTYLE-related considerations

MOBISTYLE deals with a complex information management that might include information on behavior of MOBISTYLE participants. Information collected from sensors might indicate personal behaviors. As a consequence, definition of information flows and possible archetypes of the MOBISTYLE legal model, need to address first the complexity of IoT data, data collection and management in respect to GDPR.

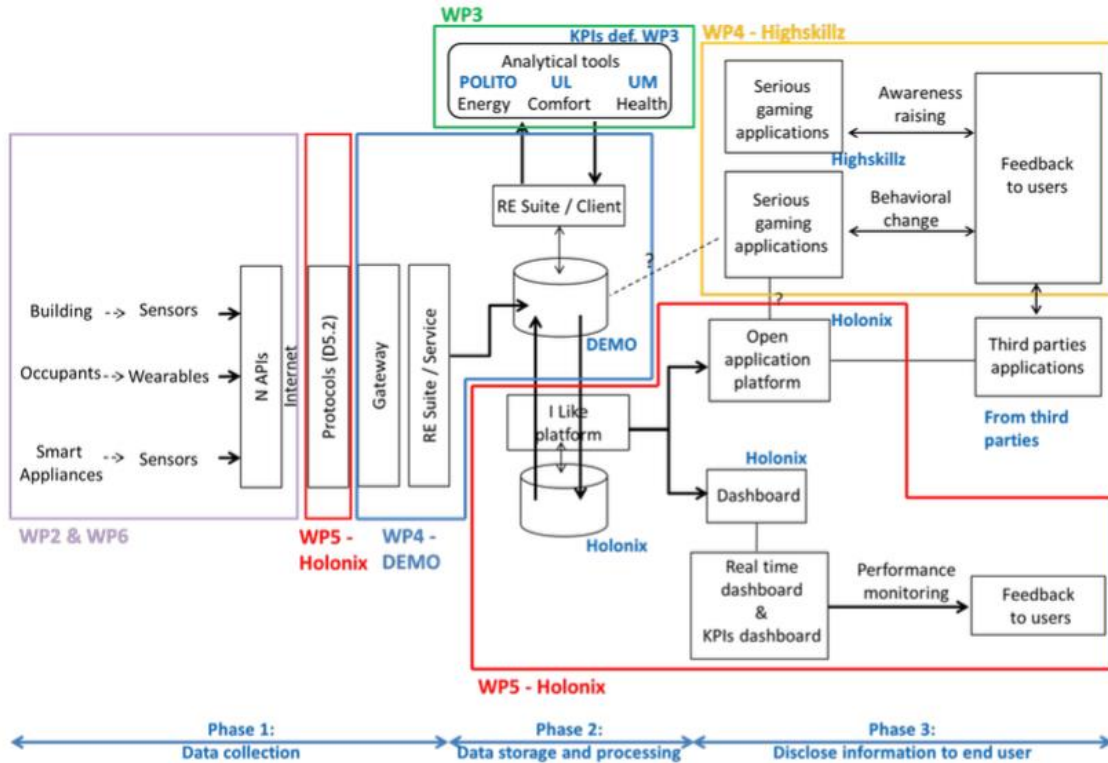


Figure 5: An initial schema of the MOBISTYLE distributed system (D4.2) relevant for identification of the GDPR specific actors and requirements.

Figure 5 exemplifies who are the actors in the general structure of the MOBISTYLE distributed system that enables information flow between the data controllers and data subjects (i.e. customers and users of MOBISTYLE services). This schematic representation of the MOBISTYLE system architecture went through certain modifications along the implementation phase due to some strategic changes aimed at improving performance of the data flows. For instance, a very recent upgrade includes migration of the DEMO database into the Azure Cloud. Accordingly, task T5.2 has enhanced its attention to the harmonisation of on-going legislative, contractual, and technical changes with the on-going technical developments of the MOBISTYLE platform as to ensure that access to the collected information does not compromise any personal data. In particular, the roles and responsibilities of individual project partners, taking care of personal data collection and processing in their local databases (e.g. local databases at the demonstration sites are not depicted in Figures 5), following the GDPR requirements, need to be identified and incorporated in a more comprehensive framework for the MOBISTYLE personal data management and processing.

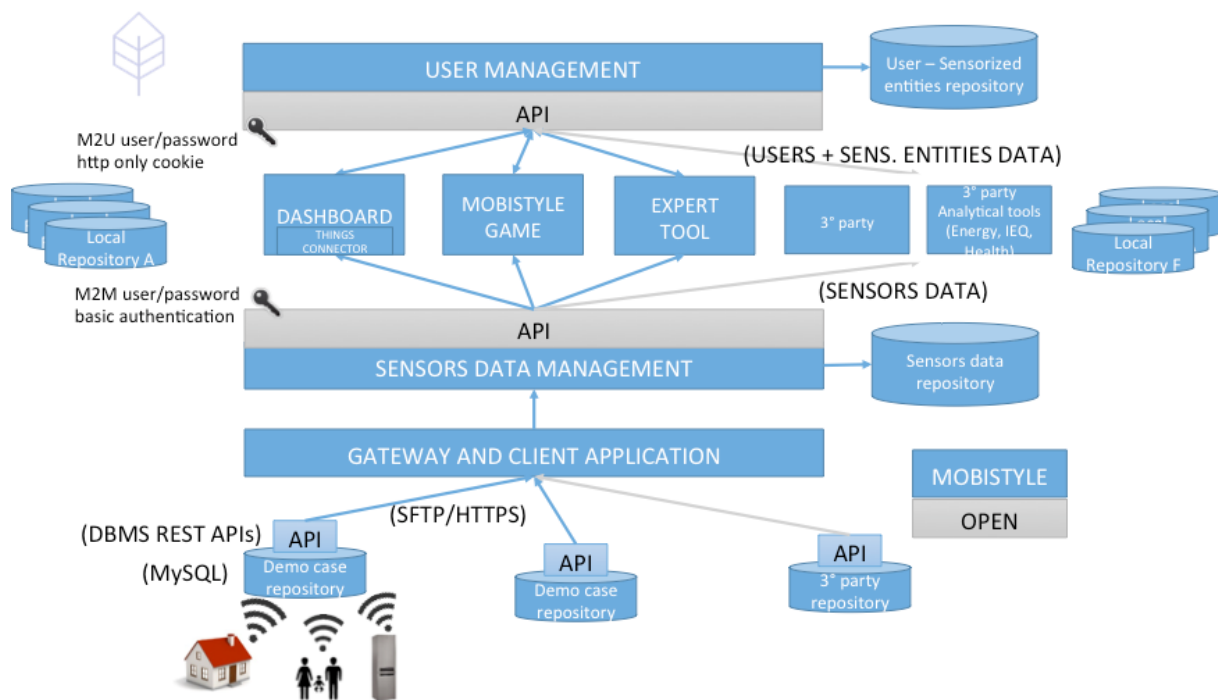


Figure 6: The basic architecture of the MOBISTYLE platform.

Also, ongoing technical and functional decisions on the forthcoming developments related to the Open Platform will have to be considered in the light of the GDPR requirements, as the Platform should provide access to the 3<sup>rd</sup> parties without compromising any personal data. The identification of roles and responsibilities (Controller, Processor, DPO, 3<sup>rd</sup> party, etc.) as well as a feasibility study will be the curtail point towards a sustainable implementation of the GDPR directives as well as a continuous and synchronized engagement in the privacy safeguarding.

## 9. A GDPR-related mapping within MOBISTYLE

In phase two of the MOBISTYLE action plan (Section 1), a workshop will be conducted under the guidance of a legal expert. The main expected outcomes of the workshop (phase 2) is assignment of responsibilities and appointment of Controller(s), Processors(s) (Section 5), as well as identification of personal data that should be safeguarded according to the requirements of GDPR (Sections 6-7). This activity will include elaboration of risks and preventive measures to reduce risks to personal data disclosure.

GDPR obliges Controllers to perform a Data Protection Risk Assessment. In addition, a Data Protection Impact Assessments might be required when certain types of processing of personal data are likely to present a high risk to the data subject. This assessment should include a systematic and extensive evaluation of organization’s processes, possible profiles, and how the employed tools safeguard the personal data.

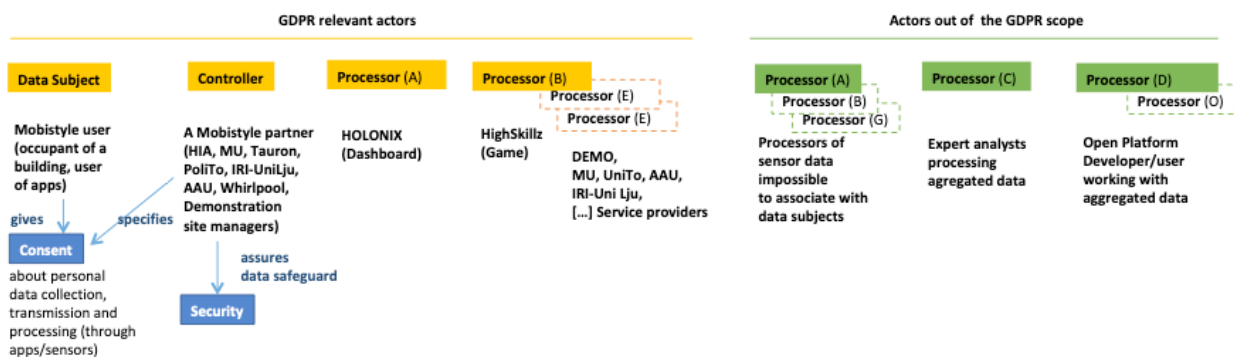


Figure 7: The initial role-mapping and possible directions towards identification of GDPR-related actors in MOBISTYLE.

Figure 7 depicts an initial mapping of possible roles and responsibilities of actors involved in MOBISTYLE, either as data Subjects, or as the data Controllers and Processors. This is just an initial consideration that is going to be discussed and revised in the light of the interactions between the consortium partners and legal experts. However, it provides some initial thoughts, mostly distinguishing actors dealing with personal data and those who deal with data associated with sensors that cannot be directly linked to individual persons, thus belong out of the GDPR scope. The figure also communicates that some actors might be involved in both, processing of personal data as well as non-personal data coming from the sensors that cannot relieve any information about data subjects. An open question that should be analyzed with the legal experts and MOBISTYLE partners includes considerations on what data should be considered as possibly associated with individual users of the facilities.

The mapping is also open to changes in respect to the ongoing development of the data apps, storage solutions, communication protocols, and definition of functionalities of the Open Platform providing access to the 3<sup>rd</sup> parties.

These as well as other open issues presented along this report will be addressed in the second and third phase (Sections 1 and 10) of the trust and privacy analysis.

## 10. The action plan timeline and concluding remarks

The document introduced some basic concepts and requirements of GDPR that should be addressed within the MOBISTYLE project as it deals with collection and processing of personal data. A list of actions, mandatory and optional activities, relevant for the implementation and assessment of GDPR compliance was introduced.

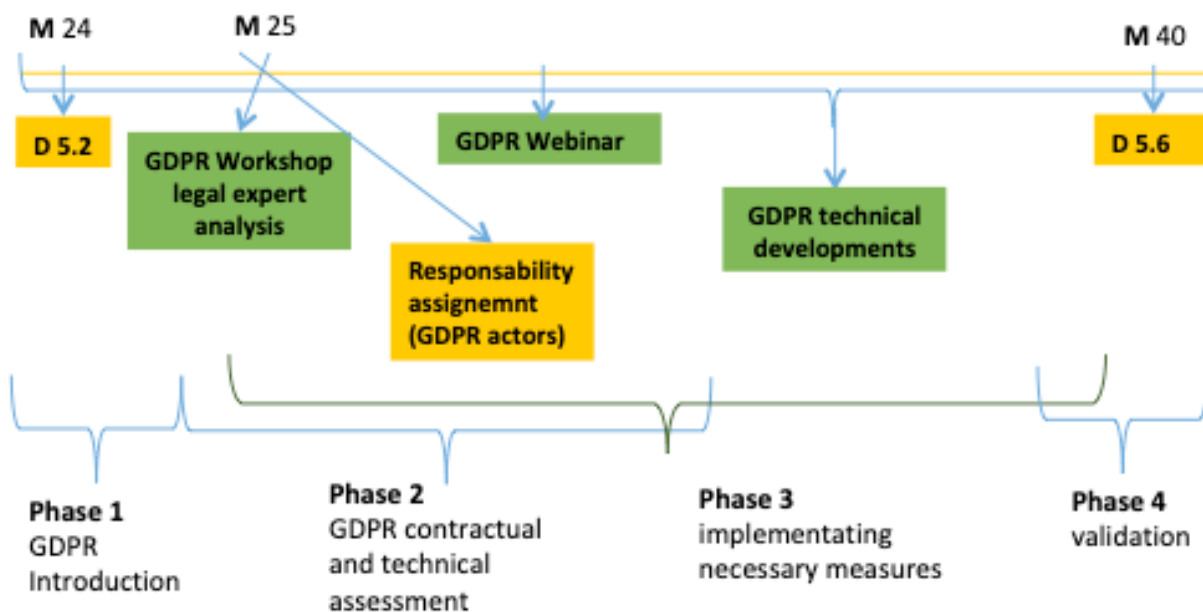


Figure 8: The action plan timeline for the GDPR compliance definition and implementation in MOBISTYLE.

An in-depth analysis of the MOBISTYLE specific requirements will follow the four phases action plan (Figure 8) presented in Section 1. The second phase will host a workshop between IT partners and a legal expert, with the aim to identify responsibilities assigned to the partners who either collect or process personal data of the MOBISTYLE users (Section 9, Figure 7). Once these aspects have been analysed, a webinar will be organised, to report the outcomes to the other partners, in particular to the use case owners, that will have a key role in the identification of measures to give informed consent to the final users. The forthcoming activities on each demonstration site as well as further technical specification of the MOBISTYLE platform will be conducted during the phase three in order to implement all possible and feasible measures to assure trust and privacy of the users of MOBISTYLE tools and services. The final activity, performed during the phase four will result in Deliverable 5.6 that will report how and to what extent the GDPR compliance is achieved. The expected results may be used to inform other similar projects on the lessons learnt and methods used to face the issues of trust and privacy.



## References

- [1] 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), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1465486284935&from=en>
- [2] Osterman Research, GDPR Compliance and Its Impact on Security and Data Protection Programs, in An Osterman Research White Paper. 2017. p. 17.
- [3] GDPR Consent Guidance, Information Communication's Office (ICO), <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>
- [4] Nymity framework <https://info.nymity.com/gdpr-compliance-toolkit>

Annex 1

Figure 9 created by teachprivacy.com illustrates in a simple and intuitive way the key concepts and roles of GDPR introduced in this document.

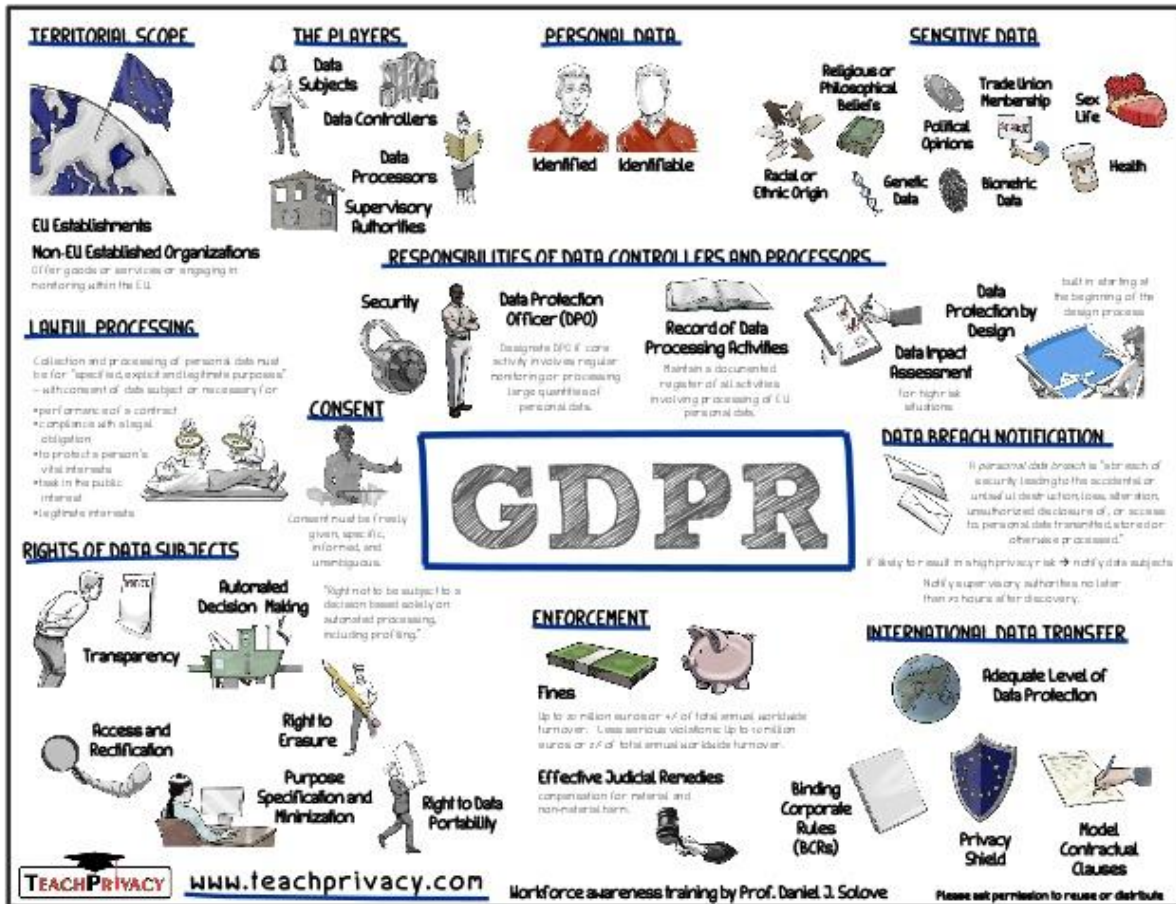


Figure 9: An illustration of basic elements of GDPR ([www.teachprivacy.com](http://www.teachprivacy.com))