



PROTECTION OF PERSONAL DATA REPORT

D11.4: PROTECTION OF PERSONAL DATA REPORT.

Date: **30/04/2020**

Author(s): **Anne Freiberger**

Co-author(s): **Julia Schmidt, Felix Nowack, Fanny Knoll, Hermann Blümel**



This project has received funding from
the European Union's Horizon 2020
research and innovation programme
under grant agreement No [875187]



Deliverable details

Project number	Project acronym	Project title
H2020 - 875187	USER-CHI	Innovative solutions for USER centric Charging Infrastructure

Title	WP	Version	Responsible Partner
D11.4 Protection of personal data report	11	1.0	IKEM

Contractual delivery date	Actual delivery date	Delivery type*
M3 (April 2020)	M3 (April 2020)	ETHICS-PU

*Delivery type: **R**: Document, report; **DEM**: Demonstrator, pilot, prototype; **DEC**: Websites, patent fillings, videos, etc.; **OTHER**; **ETHICS**: Ethics requirement; **ORDP**: Open Research Data Pilot.

Author(s)	Organisation
Anne Freiberger	IKEM
Julia Schmidt	IKEM
Felix Nowack	IKEM
Fanny Knoll	IKEM
Hermann Blümel	IKEM
	ETRA (information included from D12.1)

Document history

Version	Date	Person	Action	Status*	Dissemination level**
V0.1	14 April 2020	Anne Freiberger	First Draft of D11.4	Draft	PU
V0.2	27 April 2020	Richard Kemmerzehl	Review	Draft	PU

V0.3	28 April 2020	Maria Tomas	Content and format review	Draft	PU
V1.0	30 April 2020	Anne Freiberger	Final Editing	Final	PU

*Status: Draft, Final, Approved, Submitted (to European Commission).

Dissemination Level: **PU: Public; **CO**: Confidential, only for members of the consortium (including the Commission Services); **EU-RES** Classified Information - restraint UE; **EU-CON**: Classified Information - confidential UE; **EU-SEC**: Classified Information - secret UE

Abstract

This report describes the actions conducted to protect the personal data collecting and processing process from an ethical point of view. In this regard, detailed information will be outlined for the procedure of data collection, as well as storage, protection, retention and destruction. Moreover, the confirmation that the procedure complies with national and EU laws will be developed. Finally, it contains the templates and documents regarding personal data usage.

Keywords

Ethics, procedures, requirements, personal data, data protection, data security, informed consent, legislation

Copyright statement

The work described in this document has been conducted within the USER-CHI project. This document reflects only the USER-CHI consortium view and the European Union is not responsible for any use that may be made of the information it contains.

This document and its content are the property of the USER-CHI consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the USER-CHI Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the USER-CHI Partners.

Each USER-CHI Partner may use this document in conformity with the USER-CHI Consortium Grant Agreement provisions.

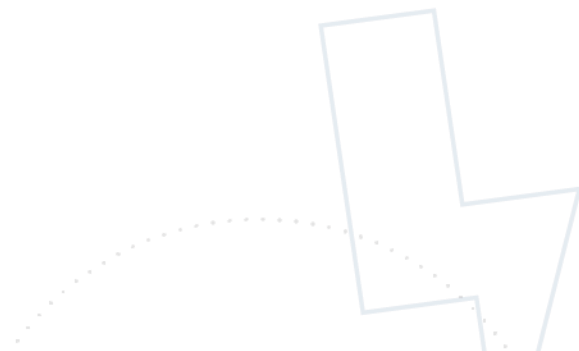
Executive summary

The objective of this document is to describe actions, which need to be implemented by the project partners of the USER-CHI consortium, that are involved in proceeding personal data of research participants. The actions outlined are needed from an ethical point of view in order to foster the protection of the personal data of the research participants throughout the collection and processing process.

D11.4 is the outcome of WP11- Task 11.3 “Data Management and Protection and IPR strategy”. The main objective of this task is to provide a data management plan (DPM). However, the data management plan will be provided within D11.3 after project month 6.

The aim of D11.4 is to provide detailed information on the procedures for personal data collection, storage, protection, retention and destruction. In addition, the conformation, that all research activities undertaken in USER-CHI comply with national and EU legislation will be developed.

A Template, which provides a “Check-List” for USER-CHI project partners will be included in the Report, in order to assist the project partners in applying the necessary personal data protection requirements.



List of abbreviations

BDSG	German Federal Data Protection Act
CFR	Charter of Fundamental Rights of the European Union
EU	European Union
EV	Electric Vehicle
GDPR	General Data Protection Regulation
IT	Information Technology
TEU	Treaty of the European Union



Table of Contents

1.	Introduction	7
1.1.	<i>Aim of the document</i>	7
1.2.	<i>Scope of the document</i>	7
1.3.	<i>Structure of the document</i>	8
2.	Ethical viewpoint on personal data collection and processing.....	9
2.1	<i>Ethics in research</i>	9
2.2	<i>Scope of relevant human rights legislation.....</i>	11
2.1.2	<i>The Charter of Fundamental Rights of the European Union (CFR)</i>	12
2.2.2	<i>The European Convention on Human Rights (ECHR)</i>	13
3.	The General Data Protection Regulation (GDPR)	15
3.1	<i>Material Scope of the GDPR</i>	15
3.2	<i>Controllers of processing procedures of personal data</i>	17
3.3	<i>Overview of relevant GDPR principles for data collection and processing.....</i>	18
3.2.1	<i>Informed Consent.....</i>	18
3.2.2	<i>Principle of Data minimization</i>	19
3.3.3	<i>Principle of storage limitation.....</i>	21
3.3.4	<i>Principle of integrity and confidentiality</i>	22
3.3.5	<i>Duty to undertake a data protection impact assessment</i>	23
4.	Technical and organizational measures	25
4.1	<i>Grant Agreement Requirements.....</i>	25
4.2	<i>Technical and organizational measures in accordance with Art. 24 GDPR</i>	26
4.3	<i>Technical and Organizational Measures according to Recital 78 (GDPR)</i>	28
4.4	<i>Conformity with European and national data protection legislation</i>	29
5.	Templates regarding the use of personal data.....	31
5.1	<i>Template – Checklist for the proceeding of personal data</i>	31
6.	Conclusions.....	34
7.	References	36

1. Introduction

USER-CHI aims to foster the deployment and market acceptance of EVs in Europe by conducting user-centric research. Therefore, it is foreseen to develop and demonstrate eight USER-CHI products in the context of seven specific applications in five demonstration sites (Barcelona, Berlin, Budapest, Rome and Turku) and two replication sites (Murcia, Florence). Accordingly, the engagement with end users and stakeholders is a key component for USER-CHI.

1.1. Aim of the document

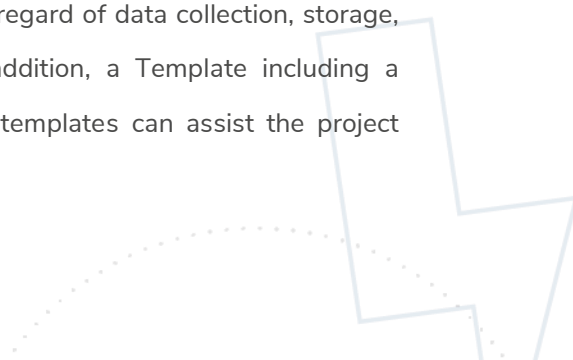
The engagement of humans will be subject to USER-CHI throughout the whole project. In particular, humans will be involved in surveys, interviews, focus group and observational studies and will be particularly addressed in work carried out within WP1 and WP6. Both WPs focus on analyzing end user requirements, motivations and constraints of participation, as well as planning, coordinating and organizing the pilot activities.

1.2. Scope of the document

The report will provide a description of necessary actions that need to be conducted by the project partners, in order to safeguard the rights of the research participants throughout USER-CHI from an ethical point of view.

The ethical requirements for the protection of personal data of research participants are rooted within data protection laws – namely the GDPR on the European level. Therefore, relevant principles and definitions of the GDPR will be explained, in order for the project partners to understand the scope.

Moreover, practical technical and organizational measures in regard of data collection, storage, protection, retention and destruction will be outlined. In addition, a Template including a “Checklist” for the project partners will be developed. The templates can assist the project partners to act in accordance with GDPR requirements.



1.3. Structure of the document

The report comprises six chapters. Following the introduction, the second chapter gives an overview of relevant international and European human rights legislation, which forms a basis for the ethical requirements for the involvement of humans in research practices.

The third chapter outlines definitions and principles of the GDPR. As all research activities of the project partners fall within jurisdictions of European Member States, the GDPR is the major applicable regulation for the protection of personal data. Therefore, the material scope of the GDPR will be presented, in order for the project partners to be able to evaluate the applicability of the GDPR towards their research activities. Relevant definitions of the terms “personal data”, “proceeding of data” and “controller” will be outlined.

Furthermore, the general principles of the requirement of informed consent, the data minimization principle and the limitation storage principle will be explained. Besides the principle of integrity and confidentiality, as well as the possibility of the duty to undertake a data impact assessment for certain research activities, will be outlined.

In addition, the fourth chapter provides an overview of technical and organizational measures for the procedure of data collection, storage, protection, retention and destruction. Furthermore, this chapter contains the confirmation for project partners to act in conformity with EU and national data protection laws.

Following to which, the fifth chapter provides a template for the usage of personal data in form of a checklist. This template summarizes duties and requirements, which have to be applied by project partners who proceed personal data of research participants.

Finally, the last chapter provides conclusions and the most relevant synergies with other deliverables within USER-CHI. Those synergies are mainly found in WP1, WP6, WP11 and WP12.

2. Ethical viewpoint on personal data collection and processing

This chapter provides an overview of the meaning of ethics in research with a special focus on ethical issues most relevant for the USER-CHI project. It explains fundamental principles of research integrity and explores why reliability, respect and accountability are of special importance for USER-CHI.

Moreover, the second chapter establishes an overview of relevant international and European human rights legislation, which builds a basis for an analysis of ethical issues in USER-CHI.

2.1 Ethics in research


Ethics are an important aspect of research projects from the start. Ethical principles and legislation need to be applied to all fields of scientific research: for example, biomedical research, as well as social sciences and humanities.¹ Hence, ethical requirements need to be taken into account by the USER-CHI consortium as well.

Therefore, this chapter will provide an overview of common ethical issues in research, as well as ethical guidelines, which help to address the issues and set out certain rules of adequate research actions.

Ethical issues, which are the most common in research cover:

- *“the involvement of children, patients, vulnerable populations,*
- *the use of human embryonic stem cells,*
- *privacy and data protection issues,*

¹ European Commission, “Horizon 2020 Programme -Ethics”,
<<https://ec.europa.eu/programmes/horizon2020/en/h2020-section/ethics> >, accessed 15 April 2020.



- *research on animals and non-human primates*²

The relevant ethical issue, which this report helps to address are privacy and data protection issues. Privacy and data protection issues may arise within USER-CHI as part of the project partners proceed with personal data from research participants for a variety of different reasons. The relevant research activities, which include research participants will be mainly undertaken in WP1 and WP6.

Moreover, the *European Code of Conduct for Research Integrity* offers legal, ethical and professional responsibilities for research activities.³ Even though different fields of researcher are using different methods, they share the goal of obtaining knowledge and understand the world we live in.⁴

The fundamental principles of research integrity are:

- **„Reliability** in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.
- **Honesty** in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.
- **Respect** for colleagues, research participants, society, ecosystems, cultural heritage and the environment.
- **Accountability** for the research from idea to publication, for its management and organization, for training, supervision and mentoring, and for its wider impacts.⁵

Those fundamental principles need to be followed by the USER-CHI consortium in all stages of the project.

² European Commission, “Horizon 2020 Programme -Ethics”, <<https://ec.europa.eu/programmes/horizon2020/en/h2020-section/ethics> >, accessed 15 April 2020.

³ ALLEA- All European Academies, “The European Code of Conduct for Research Integrity”, Revised Edition, 2017, p.3.

⁴ ALLEA- All European Academies, “The European Code of Conduct for Research Integrity”, Revised Edition, 2017, p.3.

⁵ ALLEA- All European Academies, “The European Code of Conduct for Research Integrity”, Revised Edition, 2017, p.5.

Regarding the topic of the usage of personal data, which is addressed within D11.4, the most relevant fundamental principles, which need to be followed are:

- *Reliability, Respect and Accountability*

Concerning *reliability* in ensuring the quality of research, the principle of “privacy by default” or “privacy by design” needs to be taken into account, while developing software for end-users.

The principles of privacy by design and by default will be further explored in *sub-section 4.3* of this report.

Moreover, the fundamental principle of *respect* needs to be applied throughout all interactions with research participants. The communication should be transparent, polite and dedicated in order to guarantee, that research participants feel respect, understood and safe at all times, while taking part in research activities.

At last, the fundamental principle of *accountability* needs to be implemented by the project partners in regard to personal data usage. The personal data management should be a planned process, which takes into account all the necessary actions in order to protect the personal data of research participants.

2.2 Scope of relevant human rights legislation

For the purpose of creating a deeper understanding of relevant legislation for ethical issues in research, this chapter provides an overview of relevant international, European and national legal texts. The description of the scope and meaning of legislative sources will integrate the ethical requirements in a wider legal framework.

- **Both ethical duties and legal duties build synergies and can influence each other**

Those synergies can be described as follows:

“Ethics is not fully covered by legal regulation. This means that not every issue that is relevant from an ethical perspective could and should be legally regulated. On the other hand, sometimes the reason behind legal regulation is merely pragmatic. However, laws must always reflect on

ethical implications and fulfil ethical demands. Therefore, ethical guidelines and principle do not render legal regulation unnecessary.”⁶

The Regulation (EU) No 1291/2013 on the establishment of the Horizon 2020 Programme clarifies the synergies between ethical principles and legislation further.

Article 19 on “Ethical Principles” states:

- All the research and innovation activities carried out under Horizon 2020 shall comply with **ethical principles** and **relevant national, Union and international legislation**, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols.

Particular attention shall be paid to the **principle of proportionality**, the **right to privacy**, the right to the **protection of personal data**, the right to the physical and mental integrity of a person, **the right to non-discrimination** and the need to ensure high levels of human health protection.

For the purpose of creating a deeper understanding of the legal framework for ethical research, this chapter provides an overview of the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights, as well as the [General Data Protection Regulation \(GDPR\)](#).

In addition, it will offer information on national data protection laws.

Furthermore, the USER-CHI consortium takes into account any legal guidelines regarding ethical conducts within the countries involved with the project, which are not further outlined in this document.

2.1.2 The Charter of Fundamental Rights of the European Union (CFR)

This sub-section explores the nature of the Charter of Fundamental Rights of the European Union (CFR) and provides an overview of relevant fundamental rights arising out of the CFR for research participants.

⁶ *Datenethikkommission der Bundesregierung Bundesministerium des Innern, für Bau und Heimat/Bundesministerium der Justiz und für Verbraucherschutz (Editors), „Kurfassung des Gutachten der Datenethikkommission der Bundesregierung“, (“Short version of the Report of the commission of data ethics”), 2019.*

The CFR builds an important basis for the ethical requirements of research. It is a legally binding instrument, which codifies the fundamental rights in the European Union's legal order.⁷

More details about the CFR and its status as European Law are included in D11.2.

The relevant Article of the CFR for personal data collecting from research participants and further processing procedures is:

- **Article 8 – Protection of Personal Data**

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

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

2.2.2 The European Convention on Human Rights (ECHR)

This sub-section explores the nature of the European Convention on Human Rights (ECHR) and provides an overview of relevant human rights arising out of the Convention for research participants.

The ECHR was established as the first convention of the Council of Europe, which is an international organization. The implementation of the ECHR is overseen by the European Court of Human Rights. Moreover, the ratification of the Convention is a pre-requirement in order to join the Council.⁸

The relevant Article of the ECHR for personal data collecting from research participants and further processing procedures is:

- **Art. 8 Right to Privacy**

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

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-

⁷ European Parliament, Fact Sheets on the European Union, "The Charter of Fundamental Rights", 2017, p.1.

⁸ Council of Europe, "A convention to protect your rights and liberties", <<https://www.coe.int/en/web/human-rights-convention/home>>, accessed 15 April 2020.

being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.



3. The General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), was established in order to protect individuals regarding the free movement of their personal data as well as the processing of it.⁹ The directive entered into force in 2016 and is applicable since 2018.¹⁰

The regulation is an important improvement in the field of personal data protection in comparison to the former fragmentation in different national law systems.¹¹ It strengthens individual's fundamental rights in the age of digitalization.¹²

Since national data protection laws can be relevant for certain personal data proceedings and overview of national data protection laws is included in [D11.2](#) and [D12.1](#). However, since the subject of personal data protection has been harmonized for all European member states through the GDPR this legislation of major importance will be presented in the following sub-sections.¹³

IKEM is not allowed to give legal advice. Therefore, IKEM cannot make final statements on the classification of legally significant roles and requirements under the GDPR. However, this report can provide an assessment that can help the project partners to understand the possible scope of their legal responsibilities.

3.1 Material Scope of the GDPR

This sub-section presents the material scope of the GDPR briefly.

The material scope of the Directive is defined in Art. 2 GDPR. Art. 2 (1) of the GDPR states that, the

⁹ European Commission, "Data Protection in the EU", <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>, accessed 15 April 2020.

¹⁰ European Commission, "Data Protection in the EU", <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>, accessed 15 April 2020.

¹¹ European Commission, "Data Protection in the EU", <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>, accessed 15 April 2020.

¹² European Commission, "Data Protection in the EU", <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>, accessed 15 April 2020.

¹³ European Commission, "Data Protection in the EU", <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>, accessed 15 April 2020.

- this Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Moreover, personal data is defined in Art. 4 (1) GDPR as:

- (...) 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.

The research activities, which are planned in WP1 and WP6 could potentially involve a variety of personal data. This could include names, gender, email addresses, use of electric cars, use of charging infrastructure, use of mobile app devices etc.

As long as this information can be related to an identified or identifiable natural person, in this case, the research participants, this information is regarded as personal data.

An important aspect, which renders the scope of the GDPR not applicable is the process of anonymization of former personal data.

Recital 26 of the GDPR states that,

- *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. 6This Regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes.*

However, it is likely that personal data will be anonymized at a later stage of the research project, as long as anonymization is not possible from the beginning. Therefore, it is important to apply the GDPR towards personal data, that has not been anonymized yet.

In addition, the term processing is defined in Art. 4 (2) GDPR as:



- „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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.“

The planned research activities, which are undertaken in WP1 and WP6, will at least involve the collection, organization and storage of personal data in order to use it for research purposes. The data will be analyzed through different methods in order to provide results, which are needed for the project goal.

Therefore, some research activities will be regarded as “processing personal” data.

Conclusively, the GDPR will be applicable to those research activities.

In order to act in compliance with the GDPR regulation, the project partners which are involved in processing data need to meet the requirements arising out of it.

3.2 Controllers of processing procedures of personal data

This sub-section describes the definition of the “controller” of processing procedures of personal data, which is set out in Art. 4 GDPR. The role of the controller is an important aspect of the GDPR, as certain responsibilities arise out of this role.

Art. 4 (7) GDPR explains that,

- *‘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.*

Concerning the USER-CHI research activities the project partners who process personal data, will likely be regarded as controller.

Therefore, they have to meet responsibilities, which arise out of this role.

Art. 24 GDPR presents the responsibilities of the controller:

- 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
- 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
- 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Most importantly Art. 24 No.1 GDPR determines, that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

In order to help the project partner to meet those requirements, [Chapter 4](#) of this report will analyze the technical and organizational measures needed to provide necessary protection of personal data.

3.3 Overview of relevant GDPR principles for data collection and processing

This sub-section will provide an overview of important principles, which derive under the GDPR. Therefore, this sub-section will describe in detail:

The informed consent process, the principle of data minimization, the principle of storage limitation, the requirement of integrity and confidentiality, as well as the duty to undertake a data protection impact assessment for specific activities.

3.2.1 Informed Consent

The duty to apply the informed consent procedure applies at the first stage of the data proceeding process: the data collection.

[D11.2](#) deals with the detailed procedure on the involvement of research participants. It also explains why the process of informed consent for research participants is necessary from an

ethical point of view. Moreover, [D11.2](#) gives guidelines for the project partners on how to implement the informed consent procedure in USER-CHI correctly.

However, the GDPR describes the requirement of informed consent for any kind of proceeding of personal data.

The requirement of the individual's consent in order to process personal data is established in Art. 7 GDPR.

Art. 7 (1) GDPR states that,

- where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Furthermore, Art. 7 (2) GDPR requires that,

- if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Recital 32 of the GDPR outlines that,


- consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

The project partners of USER-CHI should keep the copies of the Template I (Information Sheet) and Template II (Informed Consent) included in [D11.2](#) on file, in order to be able to meet the requirement set out in Art. 7 (1) GDPR.

In addition, the requirement of Art. 7 (2) GDPR can be met by using the Template I and II provided in [D11.2](#) as well.

3.2.2 Principle of Data minimization

This sub-section describes the principle of data minimization according to Art. 4 I GDPR.



It is necessary, that a data minimization policy will be adopted at all levels of the project and will be supervised by each responsible pilot demonstration. The principle of data minimization is relevant for the first stage of the proceeding of data: *the data collection*.

The confirmation of the application of the data minimization principle will be provided by the project partners and will be part of D12.2.

The confirmation template, which is provided within D12.2, describes the principle of data minimization as follows:

While applying the principle of data minimization you have to guarantee that irrelevant personal data is not collected.¹⁴

Art. 4 (1) GDPR defines personal data as “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.”

One of the key principles of the GDPR is the principle of data minimization. The principle of data minimization is defined in Art. 5 No. 1 c) GDPR, where it states that (...) where personal data is needed, it should be adequate, relevant, and limited to what is necessary for the purpose (‘data minimisation’).

Recital 39 of the GDPR describes that the principle of data minimization (...) requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Example:

An example for the distinction between data which can be reasonably collected, and data, that should not be collected due to the lack of added value for the project goals is given below:

- *USER-CHI wants to foster the potential of electromobility in Europe. The project puts the users in the centre and wants to explore their needs. As gender plays a role for analyzing needs in the transport sector the data can be used to analyze gender-driven needs.¹⁵ On the other hand, religious beliefs of research participants are likely not to be relevant in order to reach the goals of the project.*

¹⁴ European Commission, *Principles of the GDPR – How much data can be collected?*, <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-much-data-can-be-collected_en>, accessed 15 April 2020.

¹⁵ European Institute for Gender Equality, *Transport – Relevance of gender in the policy area*, <<https://eige.europa.eu/gender-mainstreaming/policy-areas/transport>>, accessed 15 April 2020.

The following questions can help the project partners to apply the principle of data minimization towards their own research activities:

- *What do you want to explore by asking the research participants for this specific data?*
- *How is this relevant for the project's goal?*
- *Could the purpose of the processing be fulfilled by other means?*

In case any questions arise in order to determine, which data to collect, the project partner can contact *IKEM* in their role of *Ethics Advisor* within the USER-CHI project.

3.3.3 Principle of storage limitation

This subsection describes the principle of storage limitation of personal data.

The storage limitation takes up the purpose limitation of the processing and supplements this with the requirement that the connection to certain personal data may only exist as long as this is necessary for the purpose of the proceeding in the first place.¹⁶

Art. 5 No.1 (e) GDPR states that, 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; 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');*

The principle of storage limitation will be outlined in the *Data Management Plan (D11.3)*.

Moreover, the Grant Agreement (No. 875187), of the USER-CHI project already states that,

¹⁶ Paal, Boris/ Pauly, Daniel A. (Editors), *Beck'sche Kompakt-Kommentare, Datenschutzgrundverordnung – Bundesdatenschutzgesetz, 2. Edition 2018, Art.5, Rn.43.*

- *unless specifically requested and agreed any collected data will be destroyed within 12 months of the completion of the project to allow for end of project dissemination and follow-up.*¹⁷

3.3.4 Principle of integrity and confidentiality

This subsection describes the requirement of “Integrity and confidentiality”, which are established under the GDPR.

Art. 5 No.1 (f) states that,

- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').*

The “technical and organizational measures” describes in [Chapter 4](#) of this report can help the project partners of USER-CHI to meet the requirements of integrity and confidentiality.

Art. 32 GDPR further develops on the concept of “technical and organisational” measures, which are needed to ensure a high level of security. In accordance to Art. 32 GDPR those measures may include:

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

Recital 39 clarifies, that the measures to provide security and confidentiality, need to include,

- *preventing unauthorized access to or use of personal data and the equipment used for the processing.*

¹⁷ Grant Agreement No. 875187, p. 119.

In conclusion, the project partners of USER-CHI, which are proceeding personal data, need to adopt appropriate measures in order to implement the principle of “integrity and confidentiality.”

3.3.5 Duty to undertake a data protection impact assessment

This sub-section analyses the duty to undertake a data protection impact assessment for specific types of processing personal data.

Art. 35 No.1 GDPR states that,

- *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, 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.*

(...)

The requirement of a high risk needs to be understood as the high risk of damages for the rights and freedoms of natural persons.¹⁸ Within the USER-CHI project and research activities no high risks for the damages of rights and freedoms of research participants can be foreseen at this point.

In addition, Art. 35 No.3 GDPR clarifies, that

- *A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
 - (a) 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 significantly affect the natural person;*
 - (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
 - (c) a systematic monitoring of a publicly accessible area on a large scale.*

¹⁸ Paal, Boris/ Pauly, Daniel A. (Editors), Beck'sche Kompakt-Kommentare, Datenschutzgrundverordnung – Bundesdatenschutzgesetz, 2. Edition 2018, Art. 35 Rn. 25-27.

Moreover, the Recital No. 91 sets out, that the duty to undertake a data impact assessment

- *(..) should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights.*

The research activities planned within task 1.1. of USER-CHI, the big data analysis, might count as a large-scale processing operation. However, if the personal data of end-users will solely be analyzed after they have been anonymized the material scope of the GDPR is not applicable, which means that the requirement to undertake a data impact assessment is also not relevant for T1.1.1. Therefore, the requirement of data anonymization needs to be taken into account by the project partners who are included in T1.1.1, if the duty to undertake a data impact assessment according to Art. 35 No.3 GDPR should be precluded.

However, the other planes research activities within WP1 and WP6 do not fall within the scope of Art. 35 GDPR from the Ethics Advisor perspective.

Nevertheless, if planned research activities change within the project, and if additional proceedings become large-scale activities, or set a high risk for the rights and freedoms of research participants, the duty to undertake a data impact assessment could also arise at a later point.



4. Technical and organizational measures

This chapter explores the required technical and organizational measures for USER-CHI project partners, which are involved in proceeding personal data of research participants.

First, the technical and organisational requirements provided by the USER-CHI Grant Agreement (No. 875187) will be outlined.

Moreover, this chapter will explain additional practical actions in order to establish data security and the guarantee of the rights of the data subjects.

4.1 Grant Agreement Requirements

The Grant Agreement of the USER-CHI project outlines some requirements in regard of data safety procedures.

In order to ensure, that the personal data of research participants who wish to withdraw from the study can be located and destroyed:

- *A list of participant identities and pseudonyms will be kept on a separate secure server.¹⁹*

Moreover, the following procedures need to be implemented in regard of the collecting and processing process of personal data according to the USER-CHI Grant Agreement:

- The collected data will remain the property of each pilot site.
- The collected data will be kept securely at all times at each pilot site.
- The collected data will be kept on secure servers under the control of the research team at each pilot site.
- Anonymization techniques will be applied to protect data confidentiality.
- The raw data will not be shared but the results will be shared to facilitate cooperative research amongst the project partners.

¹⁹ Grant Agreement No. 875187, p. 119.

- Unless specifically requested and agreed any collected data will be destroyed within 12 months of the completion of the project to allow for end of project dissemination and follow-up.²⁰

4.2 Technical and organizational measures in accordance with Art. 24 GDPR

This sub-section provides an overview of the technical and organizational measures, which needs to be implemented by the project partners of USER-CHI, which proceed with personal data of research participants.

Art. 24 GDPR merely states that “appropriate technical and organizational measures” are needed to ensure in order to be able “to demonstrate that processing is performed in accordance with this regulation.”

However, Art. 24 GDPR itself does not offer a list of examples what those appropriate technical and organizational measures should look like in practice.

Nevertheless, indications for the design of the operational safety concept are provided by § 9 BDSG in conjunction with Annex 9 (old version) on the other hand, whose specifications can still be used for the interpretation of Article 24 GDPR.²¹

Examples of technical and organizational measures therefore imply:

- *“the distribution of tasks in the use of data between organizational units and between researchers/employers is explicitly defined*
- *every employee is instructed about existing obligations deriving from legal and company data protection regulations and is periodically trained in them*
- *the access authorization to data and programs and the protection of the data carriers from being viewed and used by unauthorized persons is regulated*
- *the authorization to operate electronic devices is defined and each device is secured against unauthorized operation by precautions taken with the machines or programs used*

²⁰ Grant Agreement No. 875187, p. 119.

²¹ Raschauer in: Sydow, Europäische Datenschutzgrundverordnung, 2. Edition 2018, Art. 24, Mn. 36.

- records are kept in order to ensure that the admissibility, to the extent necessary, of operations actually carried out, in particular modifications, searches and transmissions, can be traced.”²²

The responsible person must, therefore, take sufficient precautions to ensure the confidentiality of the data and prevent access by unauthorized persons.²³ Those requirements could, for example, be met by the implementation of IT-based access restrictions, such as passwords.²⁴

In addition, measure in order to secure the data against loss or destruction needs to be implemented through organizational advice. This organizational advice could be provided by guidelines for the use of electronic devices in the institutions, as well as in situations of mobile work.²⁵

Those securing measures need to take into account measures against human action (such as careless handling of media or hacking), as well as precautions against accidental events (such as material effects or power failures).²⁶

Another important aspect is, that the controller must ensure that data is not stored, changed or unlawfully passed on without authorization.²⁷

Adequate technical and organizational measures to provide compliance with the GDPR also includes measures that guarantee the necessary updating, deletion or anonymisation of data.²⁸

Furthermore, the responsible institution must ensure that the rights of access and information of research participants can be effectively exercised regardless of the processing of data.²⁹

²² Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.37.

²³ Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.38.

²⁴ Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.38.

²⁵ Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.38.

²⁶ Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.38.

²⁷ Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.38.

²⁸ Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.38.

²⁹ Raschauer in: Sydow, *Europäische Datenschutzgrundverordnung*, 2. Edition 2018, Art. 24, Mn.38.

It is important to document the compliance and data security measures, as stated in Art. 24 (1) GDPR. This could be fulfilled through the evidence of training measures and instructions of employees, as well as technical security measures.³⁰

4.3 Technical and Organizational Measures according to Recital 78 (GDPR)

This sub-section outlines the appropriate technical and organizational measures, which should be implemented by the USER-CHI project partners, which are involved in personal data proceeding processes.

Recital 78 GDPR states, that

- (...) In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.

Moreover, the Recital 78 GDPR expands on the concept of data protection by design and default.

Recital 78 GDPR states that,

- Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

The principle of data minimization is already addressed in [Chapter 3](#) of this report and the implementation is confirmed by the project partners through [D12.2](#).

Moreover, transparency on the use and proceeding for personal data will be secured through the use of the templated for informed consent provided in [D11.2](#) The research participants should be able to monitor the data proceeding. An important aspect is the possibility for the research participants to contact the researcher, who is responsible for the data proceeding activities at all time. This will be guaranteed through the use of the templates in [D11.2](#) as well, because the responsible researchers need to fill out their contact details. A copy of the templates will be

³⁰ Raschauer in: Sydow, Europäische Datenschutzgrundverordnung, 2. Edition 2018, Art. 24, Mn.38.

handed out to the research participants in order to make sure that they have received the contact details.

Furthermore, the possibility of improving security features should be reviewed by the project partners.

Additionally, Recital 78 of the GDPR addresses the process of product and application development in regard of data protection. It states 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.*

The requirements of privacy by design and by default should be taken into account in WP3 (T3.3) of USER-CHI, when INCAR (Interoperability, Charging and Parking Platform) will be developed. As INCAR will offer a range of different services for end-users of EVs the principles of privacy by design and by default should be taken into account in the development phase of the application as well. This can help the project partners to meet the personal data protection requirements during the implementation of INCAR in T3.4.

4.4 Conformity with European and national data protection legislation

The project partners of USER-CHI, which carry out data proceeding activities need to act in conformity with European and national data protection legislation. Therefore, the substance of the reports D11.2, D11.4, as well as D12.1 and D12.2, needs to be applied by the project partners.

Relevant principles, which derive out of the GDPR, which is the most important legislation regarding data protection on the European level, are set out in Chapter 3 of the Report.

Moreover, [D11.2](#) describes the procedure of informed consent from an ethical and legal perspective and assists the project partners to act in conformity with the GDPR regarding the informed consent process.

An overview of the national data protection laws is given in [D11.2](#), as well as [D12.1](#). The demo site partners should consult this overview in order to be aware of national data protection laws, which might be applicable towards their research actions.

IKEM will serve as a contact person in their role as *Ethics Advisor* in case any doubts or questions about personal data protection requirements arise.



5. Templates regarding the use of personal data

The fifth chapter provides the Templates regarding the usage of personal data.

As already referred to in Chapter 3, the template for the application of the data minimization principle is part of [D12.2](#). The template explains the meaning of the data minimization principle and assists the USER-CHI project partners in implementing the approach during the data collection process.

Moreover, as stated in Chapter 3, the template for the Informed Consent procedure is provided in [D11.2](#). In addition, the confirmation that the relevant templates for the informed consent procedure in English, as well as the intelligible language for local research participants, are kept on file will be provided within [D12.1](#).

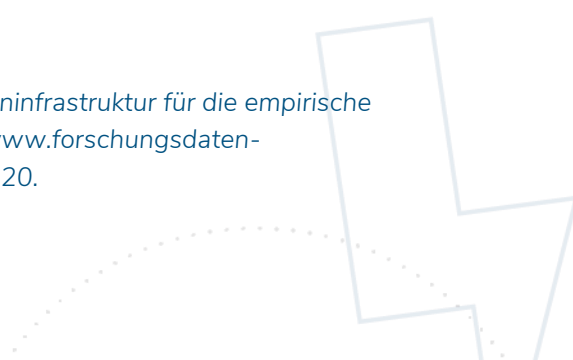
5.1 Template – Checklist for the proceeding of personal data

This sub-section provides the template: Checklist for the proceeding of personal data. This template can assist the project partners in order to implement the requirements which arise out of the GDPR while proceeding personal data.

The project partners of USER-CHI, which are involved in the proceeding of personal data, should follow this checklist step by step.³¹

-
1. On the basis of sub-section 3.1 of this report, make sure you understand the scope and meaning of personal data according to Art.4 I GDPR.

³¹ VerbundFDB - Aufbau und Gestaltung einer Forschungsdateninfrastruktur für die empirische Bildungsforschung, Informationen zum Datenschutz, <<https://www.forschungsdatenbildung.de/info-datenschutz?la=de%20>>, accessed 20 April 2020.



2. Make sure you use the Informed Consent Form and Information Sheets provided in D11.2 before processing personal data.
3. Personal data should only be collected in a scope, which is necessary for the project goals. Therefore, the data minimization principle should be implemented in accordance with the Template provided in D12.2.
4. It needs to be possible for research participants to correct or update incorrect information.
5. It must be easy for research participants to withdraw their consent to the processing of their data as well as to ask your institution to delete their personal data.
6. Collected personal data needs to be saved on secure servers.
7. No data collected will be sold or used for any purposes other than the current project, because the informed consent of the research participants only covers the scope of proceeding described in D11.2 (Template I and II).
8. Personal data should be anonymized as soon as possible during the implementation of the project.
9. Only anonymized data is allowed to be used in the report.
10. Images of the research participants are considered personal data as well and are only allowed to be used for dissemination if the participants gave their consent beforehand.
11. Only if explicitly stated otherwise the data will be deleted after 12 months of the project end.
12. Create awareness for data protection issues in your team of researchers.

13. *If necessary, collect a statement from researchers within your institutions who have access to personal data, which confirms that the principle of confidentiality will be taken into account.*

In case any questions arise, the project partners can address IKEM in its role as [Ethics Advisors](#) within the USER-CHI project.

6. Conclusions

This report describes the actions, which need to be implemented in order to protect the personal data of research participants, which is proceeded within USER-CHI research activities from an ethical point of view.

Therefore, it describes the relationship between ethics requirements and legislation on the topic of personal data protection.

Moreover, it provides an overview of the material scope of the GDPR, as well as relevant principles arising out of it. It clarifies, that the requirements of informed consent, data minimization and storage limitations need to be applied, in order to protect the rights and freedoms of research participants sufficiently. Furthermore, the report explains, that the duty to apply a data impact assessment might be necessary for big data activities, as long as personal data is not anonymized beforehand.

In addition, the report outlines the technical and organizational measures, which needs to be implemented by the project partners, which proceed with personal data of research participants. The confirmation that the research activities are carried out in conformity with European and national data protection laws is developed.

Finally, the report provides the template for a checklist for the researchers, which assists them in meeting the data protection requirements arising out of the GDPR.

The main dependencies and synergies with other deliverables are:

- *D1.1 User requirements for USER-CHI solutions:* This report will collect the user requirements analysed through the Big Data analysis and the User-Driven Innovation approach.
- *D6.1 Demonstration Concept and Implementation Plan:* This deliverable summarizes the demos' approach and focus for USER-CHI demonstrations and will specify the pilot demonstration activities with regard to technical and organizational tasks, in which the ethical requirements and defined procedures must be taken into account.
- *D11.2 Research Participant Involvement Report:* This report includes the procedures and criteria that will be used to identify and recruit research participants as well as the informed consent procedures that will be implemented for the participation of humans.

- *D11.3 Data Management Plan*: This deliverable includes information required in the guidelines on Data Management in Horizon 2020 and the data management lifecycle for the data to be collected, processed and/or generated by the project.
- *D12. 1H – Requirement No. 1*: This deliverable includes confirmation that the opinions by ethics committees or competent authorities have been obtained and are kept on file.
- *D12.2 POPD – Requirement No. 2*: This deliverable includes a description of the technical and organizational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants.



7. References

1. ALLEA- All European Academies, “The European Code of Conduct for Research Integrity”, Revised Edition, 2017
2. Council of Europe, “A convention to protect your rights and liberties”, <<https://www.coe.int/en/web/human-rights-convention/home>>, accessed 15 April 2020
3. Datenethikkommission der Bundesregierung Bundesministerium des Innern, für Bau und Heimat/Bundesministerium der Justiz und für Verbraucherschutz (Editors), „Kurfassung des Gutachten der Datenethikkommission der Bundesregierung“, (“Short version of the Report of the commission of data ethics”), 2019
4. European Commission, “Data Protection in the EU”, <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>, accessed 15 April 2020
5. European Commission, “Horizon 2020 Programme -Ethics”, <<https://ec.europa.eu/programmes/horizon2020/en/h2020-section/ethics> >, accessed 15 April 2020
6. European Commission, Principles of the GDPR – How much data can be collected?, <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-much-data-can-be-collected_en>, accessed 15 April 2020
7. European Institute for Gender Equality, Transport – Relevance of gender in the policy arear, <<https://eige.europa.eu/gender-mainstreaming/policy-areas/transport>>, accessed 15 April 2020
8. European Parliament, Fact Sheets on the European Union, “The Charter of Fundamental Rights”, 2017
9. Paal, Boris/ Pauly, Daniel A. (Editors), Beck’sche Kompakt-Kommentare, Datenschutzgrundverordnung – Bundesdatenschutzgesetz, 2. Edition 2018

10. Sydow, Gernot (Editor), *Europäische Datenschutzgrundverordnung*, 2. Edition 2018
11. VerbundFDB - *Aufbau und Gestaltung einer Forschungsdateninfrastruktur für die empirische Bildungsforschung*, *Informationen zum Datenschutz*, <<https://www.forschungsdaten-bildung.de/info-datenschutz?la=de%20>>, accessed 20 April 2020