Project Identification	
Project number	AAL-2013-6-064
Duration	1st July 2014 until 30th June 2017
Coordinator	Martin Biallas
Coordinator Organisation	Lucerne University of Applied Sciences and Arts – Engineering & Architecture, CEESAR-iHomeLab, Horw, Switzerland
Website	www.TransSafe.eu

D-2.1
Report on the ethics and legal issues

Document Identification	
Deliverable ID:	D-2.1 Report on the ethics and legal issues
Release number/date	V03: 25.02.2015
Checked and released by	MAN
Work Status	Finished
Review Status	In review

Key Information from "Description of Work"	
Deliverable Description	.
Dissemination Level	Select one: **CO=Confidential** PU=Public
Deliverable Type	R = Report
Original due date	Select one: **Not reviewed**, In Review, Request for changes, Accepted

Authorship& Reviewer Information	
Editor	MAN
Partners contributing	MAN, YOU, HSL
Reviewed by	TIL

The Project TransSafe is co-founded by the European AAL JP and the national authorities and R&D programmes from Switzerland, Germany, Italy and UK

Release History

Release Number	Date	Author(s)	Release description /changes made Please make sure that the text you enter here is a brief summary of what was actually changed; do not just repeat information from the other columns.
V01	20-10-2014	HSL	First version of Del. Template, with basic headings and suggestions for responsibilities (MAN vs. YOU)
V02	29-01-2015	YOU	Description of ethical aspects (chapter 2)
V03	25.02.2016	MAN	Description of legal aspects

Trans.Safe Consortium

Trans.Safe (AAL-2013-6-064.) is a project within the AAL Joint Programme Call 6
The consortium members are:

Partner 1	*Lucerne University of Applied Sciences and Arts – Engineering & Architecture, CEESAR-iHomeLab (Project Coordinator, HSL, CH)*
Contact person:	Martin Biallas
Email:	Martin.Biallas@hslu.ch

Partner 2	*Youse GmbH (YOU, DE)*
Contact person:	Cornelia Schauber
Email:	Cornelia.Schauber@youse.de

Partner 3	*Telecom Italia S.p.A. (TIL, IT)*
Contact person:	Gianluca De Petris
Email:	Gianluca.dePetris@telecomitalia.it

Partner 4	*VAG Verkehrs-AG Nürnberg (VAG, DE)*
Contact person:	Andreas May
Email:	Andreas.May@vag.de

Partner 5	*MAN Truck & Bus AG (MAN, DE)*
Contact person:	Walter Schwertberger
Email:	Walter.Schwertberger@man.eu

Partner 6	*Scuola Superiore Sant' Anna (SSSA, IT)*
Contact person:	Filippo Cavallo
Email:	F.Cavallo@sssup.it

Partner 7	*konplan systemhaus ag (KON, CH)*
Contact person:	Andy Tonazzi
Email:	Andy.Tonazzi@konplan.com

Partner 8	*Design LED Products Ltd (DLED, UK)*
Contact person:	James Gourlay
Email:	James.Gourlay@designledproducts.com

Table of Contents

Table of Figures

List of Tables

Abbreviations

Abbrev.	*Description*
VAG	Verkehrsbetriebe Nürnberg AG (Nuremberg Transportation System)
WMA	World Medical Association

Executive Summary

Try not to exceed one page.

Make sure that what you write really is a summary. It should not be an introduction.

Someone who reads ONLY this section should have an overall impression of all the important things contained in the document. Conversely: someone who reads all the chapters except this one should not miss anything i.e. there should be no information contained in this chapter that is contained only here.

1 About this Document

1.1 Role of the deliverable

Given the fact that for field tests personal data are captured, test persons have to be assured that these data are treated in a confidential manner. This deliverable will give an overview of guidelines for legal and ethical collection, analysis and presentation of physiological and other data necessary for Trans.Safe. MAN will elaborate legal aspects regarding advanced driver assistance systems (ADAS) with a specific focus on the term *controllability*.

1.2 Relationship to other Trans.Safe deliverables

The deliverable is related to the following Trans.Safe deliverables:

Deliv:	*Relation*
Dx.x	title: this document presents…. add a short description and make sure you explain how this document relates to it.

1.3 Structure of this document

This section is NOT mandatory. If your deliverable has a complex structure, or there are aspects of the structure that are particularly important for readers – include an overview here. If readers can easily see the structure from reading the Table of Contents, then there is no need to repeat the same information here.

2 Ethical Principles and Guidelines

2.1 Introduction to this chapter

Based on the acknowledgement that ethics, privacy and data security issues play an important role not only in general, but especially in AAL-projects, those issues have been particularly important for Tans.Safe since the beginning. This chapter will provide an overview of the legal and ethical aspects taken into account in this project and the precautionary measures taken in this project.

Trans.Safe underlies national and transnational legal requirements and internal ethic guidelines. These guidelines and regulations must be followed by all project-members in every phase of the project – collection, analysis, and presentation – where there will deal with personal data of data-subjects, users and other stakeholders.

2.2 Guidelines for handling physiological and personal data

This chapter summarizes the most important European directives and national regulations with regard to the consortium of Trans.Safe (Germany, Italy, Switzerland, Scotland). These regulations are incorporated in the Trans.Safe ethical guideline (see chapter 2.3).

2.2.1 European Regulations

The following sections list legislations of the European Union, applicable to Trans.Safe. It has to be taken into account, that a general reformation of these regulations is expected. In this section, the regulations currently effective in law are shown.

Personal Data Directive

The Directive 95/46/EC of the European Council (also known as the “Data Protection Directive”) states that personal data should not be processed at all. Exceptions can be made, for example, when the data subject has given his or her consent to the processing of the personal data (art. 7a). Furthermore, the following requirements must be met:

- Data must be processed fairly and lawfully (art. 6a).
- Data can only be collected for specified, explicit and legitimate purposes (art. 6b).
- Data collection must be proportional (adequate, relevant and not excessive) (art. 6c).
- Data must be accurate (art. 6d).
- Data must only be kept in a form allowing the identification of the data-subjects, as long as necessary for the purpose (art. 6e).
- The data subject must give his or her explicit consent to the processing of special categories of data (e.g. data concerning their health) (art. 8).
- The data-subject must receive full information about the processing of the data, including purpose, identity of the controller, recipients of the data, whether replies are obligatory or voluntary, possible consequences of failure to reply, the right of access to the data and - if necessary - the right to correct the data (art. 10).
- The data-subject’s right of access to his or her personal data must be assured (art. 12).
- Confidentiality must be ascertained (art. 16).
- The security of the processing of data must be guaranteed (art. 17).
- The supervisory authority must be notified about wholly or partly automatic processing operations (art. 18/20). This regulation can vary on national levels .
- Processing operations must be publicized (art. 21).

(cf. European Parliament/ Council of the European Union 1995)

Directive on privacy and electronic communications

The Directive 2002/58/EC (also known as the E-Privacy Directive) concerns the protection of privacy regarding the processing of personal data in the electronic communications sector.

It is a detailing and supplement of directive 95/46/EC and in particular targets the right of privacy in the electronic communication sector and free movement of data, communication equipment and services in public communication networks. The following lists the most important aspects of this directive for Trans.Safe:

- The provider must take organizational and technical security measures for its publicly available electronic communication system (art. 4, sec. 1).
- The provider must inform the user about possible safety risks and, if necessary, about solutions to these risks and their costs (art. 4, sec. 2).
- Confidentiality must be assured through in advance obtained consent of the user (consent to: "[…] listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic of data […]") (art. 5, sec. 1).
- Storage of information and access to information stored on the end-device of the user is only allowed if the user has given his or her full informed consent (art. 5, sec. 3).
- Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed (Art. 6, Sec. 2). The user must be informed about the type of data processed and about the duration of this processing (art. 6, sec. 4).
- Traffic data relating to subscribers and users processed and stored by the provider […] must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication […]" (art. 6, sec. 3)
- If the user has given his or her consent, data can be processed "[f]or the purpose of marketing electronic communications services or for the provision of value added services […]". The user can withdraw this consent at any time. (art. 6, sec. 3) The user must be informed about the type of data processed and about the duration of this processing, before giving consent (art. 6, sec. 4).
- Processing of traffic data must be restricted to persons acting under the authority of providers and must be restricted to what is necessary for the purposes of such activities (art. 6, sec. 5).

(European Parliament/ Council of the European Union 2002)

These regulations play an important role in the development, testing and market-implementation of technical devices in this project. The project-team members obligate themselves to develop a device, in compliance with this directive.

Transfer of Personal Data to Third Countries

Because of the decentralized construction of the Trans.Safe consortium, it might be necessary for personal data to travel across borders of the European Union and Switzerland.

The European Commission has determined (on the basis of Article 25(6) of the directive 95/46/EC), that Switzerland, as a third country, "ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into." Therefore, personal data can flow from the partners in Germany, Italy and Scotland to the partners in Switzerland "without any further safeguard being necessary." (European Commission 2014)

As already mentioned, in the near future broad changes are expected in the European data protection legislation. The reform is supposed to strengthen the individual rights of data-subjects, giving them more control over their personal data, especially stored on the Internet. (cf. European Commission, 2012)

If necessary, the new regulations will be integrated into the project procedure described below.

2.2.2 National regulations

The following lists a selection of important legislations in the project-member states Germany and Italy. The international project consortium (Germany, Italy, Scotland, Switzerland) has to pay special attention to Italian and German national legislation, since data is collected and mainly processed here: The observation and analysis phase (lead-user-integration, observations, interviews, group discussions and evaluation) will be run in Germany and the development and field-test of the "stress-device" (stress measurements and responses in simulations an real life situations in MAN trucks and at VAG) will be executed in Italy and Germany.

German regulations

The German Federal Data Protection Act ("Bundesdatenschutzgesetz") implements the European Directive 95/46EC into German legislation and regulates the protection of personal data of individuals and therefore the "collection, processing and use of personal data" by public and private bodies. (juris 2013)

The general principals of the directive receive specification here. The following chart lists a shortened version of the most important regulations of the federal data protection act, which will be observed by the project members:

Table 1: Regulations of the German Federal Data Protection Act, applicable to Trans.Safe

EU Directive	**Federal Data Protection Act** (original text)
Article 7a: Consent Article 8: special categories of data	**Section 4 - Admissibility of data collection, processing and use** (1) The collection, processing and use of personal data shall be admissible only […] if the data subject has consented. (2) Personal data shall be collected from the data subject. **Section 4a - Consent** (1) Consent shall be effective only when based on the data subject's free decision. Data subjects shall be informed of the purpose of collection, processing or use […]. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance. […] (3) In so far as special categories of personal data (Section 3 (9)) are collected, processed or used, the consent must further refer expressly to these data. **Section 3 (9)** (9) "Special categories of personal data" means information on a person's racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life.
Article 6a: fair and lawful processing	*Not specified in the Act.*
Article 6b: specified, explicit and legitimate purposes	**Section 28 - Collection and storage of data for own commercial purposes** (1) The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible […] 2. in so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use, […] In connection with the collection of personal data, the purposes for which the data are to be processed or used are to be stipulated in concrete terms. **Section 40 - Processing and use of personal data by research institutes** (1) Personal data collected or stored for scientific research purposes may processed or used only for such purposes.

Article 6c: Proportion (adequate, relevant and not excessive)	**Section 3a - Data reduction and data economy** Personal data are to be collected, processed and used, and processing systems are to be designed in accordance with the aim of collecting, processing and using as little personal data as possible.
Article 6d: Accuracy	**Section 35 - Correction, erasure and blocking of data** (1) Inaccurate personal data shall be corrected. Estimated data shall be clearly identified as such. (2) Personal data may be erased at any time, except in the cases specified in sub-Section 3, Nos. 1 and 2. Personal data in filing systems shall be erased if 1. their storage is inadmissible, 2. they concern information on racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health, sex life, criminal offences or administrative offences and the controller is unable to prove their accuracy, 3. they are processed for one's own purposes, as soon as knowledge of them is no longer needed for fulfilling the purpose for which they are stored, or […] (3) Instead of erasure, personal data shall be blocked where 1. in the case of sub-Section 2 second sentence No. 3 above, retention periods prescribed by law, statutes or contracts rule out any erasure, 2. there is reason to assume that erasure would impair legitimate interests of the data subject or 3. erasure is not possible or is only possible with disproportionate effort due to the specific type of storage. (4) Personal data shall also be blocked if the data subject disputes that they are correct and it cannot be ascertained whether they are correct or incorrect. (4a) The fact that the data are blocked shall not be transmitted. […] (7) The bodies to which data were transmitted for storage in the course of a data transfer process shall be notified of the correction of incorrect data, the blocking of disputed data and the erasure or blocking of data due to inadmissible storage, where this does not require disproportionate effort and the data subject has no overriding legitimate interests.
Article 6e: Data Storage and anonymity of the data subject	**Section 3a - Data reduction and data economy** […] In particular, personal data are to be aliased or rendered anonymous as far as possible and the effort involved is reasonable in relation to the desired level of protection. **Section 30 - Commercial collection and storage of data for the purpose of transfer in anonymised form** (1) If personal data are collected and stored in the course of business in order to transfer them in anonymised form, the characteristics enabling information concerning personal or material circumstances to be attributed to a identified or identifiable individual shall be stored separately. Such characteristics may be combined with the information only where necessary for storage or scientific purposes. (2) The modification of personal data shall be admissible if 1. there is no reason to assume that the data subject has a legitimate interest in his/her data being excluded from modification […] (3) Personal data shall be erased if their storage is inadmissible. **Section - 40** **Pro** […] (2) The personal data shall be rendered anonymous as soon as the research purpose permits this. Until such time the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research purpose.
Article 18/20: Notification	**Section 4d - Obligatory registration** (1) Prior to putting automated processing procedures into operation, private

	controllers of the competent supervisory authorities, public controllers of the Feration and postal and telecommunications companies shall register such procedures with the Federal Commissioner for Data Protection and Freedom of Information in accordance with Section 4e. (2) Obligatory registration shall not apply if the controller has appointed a data protection official. (3) Obligatory registration shall further not apply if the controller collects, processes or uses personal data for its **own purposes**, provided that, as a rule, **no more than nine employees are permanently employed in collecting, processing** or using personal data and either **consent has been obtained** from the data subject or the collection, processing or […] (5) In so far as automated processing operations involve risks for the rights and liberties of the data subject, they are subject to examination prior to the beginning of processing (prior checking). **Prior checking** is to be carried out in particular when 1. **special categories of personal data** (Section 3 (9)) are to be processed or 2. the processing of personal data is intended to appraise the **data subject's personality, including his abilities, performance or conduct,** unless a statutory obligation applies, the **data subject's consent has been obtained**, […] ***Section 4e Contents of the obligatory registration***
Article 10: full information	**Section 4 - Admissibility of data collection, processing and use** […] (3) If personal data are collected from the data subject, the controller is to inform him/her as to 1. the identity of the controller, 2. the purposes of collection, processing or use and 3. the categories of recipients only in so far as the circumstances of the individual case provide no grounds for the data subject to assume that data will be transferred to such recipients, unless the data subject has already acquired such knowledge by other means. […]
Article 12: right of access	**Section 6 - Rights of the data subject** (1) The data subject's right of access (Sections 19, 34) and to correction, erasure or blocking (Sections 20, 35) may not be excluded or restricted by a legal transaction. (2) If the data of the data subject are stored by means of automated procedures such that several bodies are entitled to store and if the data subject is unable to ascertain which body has stored the data, he may approach any of these bodies. Such body is obliged to forward the request of the data subject to the body which has stored the data. The data subject shall be informed of the forwarding of the request and of the identity of the body concerned. […] **Section 34 - Provision of information to the data subject** (1) At the request of the data subject, the controller shall provide information 1. on stored data about the data subject, also where they refer to the origin of these data, 2. on the recipient or type of recipients to whom the data are provided, and 3. the reason for storage. The data subject should provide a detailed description of the type of personal data he or she would like information about. […] Information about the origin and recipients may be withheld if the interest in protecting trade secrets outweighs the data subject's interest in the information. […] (5) Data stored for the purpose of providing information to data subjects pursuant to sub-sections 1a to 4 may be used only for this purpose and for data protection control; they shall be blocked for other purposes. (6) Upon request, the information shall be provided in written form, unless

	another form would be more appropriate in the circumstances. […] (8) The information shall be free of charge. […]
Article 16: Confidentiality	**Section 5 - Confidentiality** Persons employed in data processing shall not collect, process or use personal data without authorization (confidentiality). On taking up their duties such persons, in so far as they work for private bodies, shall be required to give an undertaking to maintain such confidentiality. This undertaking shall continue to be valid after termination of their activity.
Article 17: Security of data processing	**Section 9 - Technical and organizational measures** Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection. **Annex** (to the first sentence of Section 9 of this Act) Where personal data are processed or used automatically, the internal organization of authorities or enterprises is to be arranged in such a way that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or data categories to be protected shall be taken, 1. to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used (access control), 2. to prevent data processing systems from being used without authorization (access control), 3. to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage (access control), 4. to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (transmission control), 5. to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed (input control), 6. to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (job control), 7. to ensure that personal data are protected from accidental destruction or loss (availability control), 8. to ensure that data collected for different purposes can be processed separately. One measure in accordance with the second sentence Nos. 2 to 4 is in particular the use of the latest encryption procedures.
Article 21: Processing operations must be publicized	*Not specified in this Act.*

In addition, the Personal Data Protection Code includes a guideline regulating the compensation of harm, caused by the project team:

> **Section 7 - Compensation**
>
> Where a controller causes harm to the data subject through the collection, processing or use of his/her personal data that is inadmissible or incorrect under the provisions of this Act or other data protection provisions, such controller or its supporting organization shall be obliged to compensate the data subject for the harm thus caused. This obligation to provide compensation shall not apply if the controller has exercised due care in accordance with the circumstances of the case concerned.

(juris 2013)

Italian regulations

The Italian Personal Data Protection Code ("Codice in materia di protezione dei dati personali") mainly builds on the Directive 95/46/EC of the European Council and contains three parts: The first one is dedicated to general data protection principles. The second part applies to specific social and economical topics (telecommunication, healthcare, etc.) and the last part contains regulations concerning sanctions and remedies.

Furthermore the code is based on three "key guiding principles":

1. Simplification,
2. Harmonization,
3. Effectiveness.

Table 2: Regulations of the Italian Personal Data Protection Code, applicable to Trans.Safe

EU Directive	**Personal Data Protection Code** (original text)
Article 7a: Consent Article 8: special categories of data	**Section 23** *(Consent)* 1. Processing of personal data by private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent 2. The data subject's consent may refer either to the processing as a whole or to one or more of the operations thereof. 3. The data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13. 4. Consent shall be given in writing if the processing concerns sensitive data.
Article 6a: fair and lawful processing	**Section 2** *(Purposes)* 1. This consolidated statute, hereinafter referred to as "Code", shall ensure that personal data are processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection. **Section 11** *(Processing Arrangements and Data Quality)* 1. Personal data undergoing processing shall be: a) processed lawfully and fairly; […]
Article 6b: specified, explicit and legitimate purposes	**Section 11** *(Processing Arrangements and Data Quality)* 1. Personal data undergoing processing shall be: […] b) collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes; […] 2. Any personal data that is processed in breach of the relevant provisions concerning the processing of personal data may not be used.
Article 6c: Proportion (adequate, relevant and not excessive)	**Section 3** *(Data Minimisation Principle)* 1. Information systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively. **Section 11** *(Processing Arrangements and Data Quality)* 1. Personal data undergoing processing shall be: […] d) relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed; […]

Article 6d: Accuracy	**Section 11** *(Processing Arrangements and Data Quality)* 1. Personal data undergoing processing shall be: […] c) accurate and, when necessary, kept up to date; […]
Article 6e: Data Storage and anonymity of the data subject	**Section 11** *(Processing Arrangements and Data Quality)* 1. Personal data undergoing processing shall be: […] e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed. […] **Section 16** *(Termination of Processing Operations)* 1. Should data processing be terminated, for whatever reason, the data shall be a) destroyed; b) assigned to another data controller, provided they are intended for processing under terms that are compatible with the purposes for which the data have been collected; c) kept for exclusively personal purposes, without being intended for systematic communication or dissemination; d) kept or assigned to another controller for historical, scientific or statistical purposes, in compliance with laws, regulations, Community legislation and the codes of conduct and professional practice adopted in pursuance of Section 12. 2. Assignment of data in breach either of paragraph 1, letter b), or of other relevant provisions applying to the processing of personal data shall be void.
Article 18/20: Notification	**Section 26** *(Safeguards Applying to Sensitive Data)* 1. Sensitive data may only be processed with the data subject's written consent and the Garante's prior authorisation, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations. 2. The Garante shall communicate its decision concerning the request for authorisation within forty-five days; failing a communication at the expiry of said term, the request shall be regarded as dismissed. Along with the authorisation or thereafter, based also on verification, the Garante may provide for measures and precautions in order to safeguard the data subject, which the data controller shall be bound to apply. […] 4. Sensitive data may also be processed without consent, subject to the Garante's authorisation, a) if the processing is carried out for specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements by not-for-profit associations, bodies or organisations, whether recognised or not, of political, philosophical, religious or trade-unionist nature, including political parties and movements, with regard to personal data concerning members and/or entities having regular contacts with said associations, bodies or organisations in connection with the aforementioned purposes, provided that the data are not communicated or disclosed outside and the bodies, associations or organisations lay down suitable safeguards in respect of the processing operations performed by expressly setting out the arrangements for using the data 5. Data disclosing health may not be disseminated. **Section 37** *(Notification of the Processing)* 1. A data controller shall notify the processing of personal data he/she intends to perform exclusively if said processing concerns: […] e) sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive dataf used for opinion polls, market surveys and other sample-based surveys, **Section 38** *(Notification Mechanisms)*
Article 10: full information	**Section 13** *(Information to Data Subjects)* 1. The data subject as well as any entity from whom or which personal data are

	collected shall be preliminarily informed, either orally or in writing, as to: a) the purposes and modalities of the processing for which the data are intended; b) the obligatory or voluntary nature of providing the requested data; c) the consequences if (s)he fails to reply; d) the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data; e) the rights as per Section 7; f) the identification data concerning the data controller and, where designated, the data controller's representative in the State's territory pursuant to Section 5 and the data processor. If several data processors have been designated by the data controller, at least one among them shall be referred to and either the site on the communications network or the mechanisms for easily accessing the updated list of data processors shall be specified. If a data processor has been designated to provide responses to data subjects in case the rights as per Section 7 are exercised, such data processor shall be referred to. […]
Article 12: right of access	**Section 7** *(Right to Access Personal Data and Other Rights)* 1. A data subject shall have the right to obtain confirmation as to whether or not personal data concerning him exist, regardless of their being already recorded, and communication of such data in intelligible form. 2. A data subject shall have the right to be informed a) of the source of the personal data; b) of the purposes and methods of the processing; c) of the logic applied to the processing, if the latter is carried out with the help of electronic means; d) of the identification data concerning data controller, data processors and the representative designated as per Section 5(2); e) of the entities or categories of entity to whom or which the personal data may be communicated and who or which may get to know said data in their capacity as designated representative(s) in the State's territory, data processor(s) or person(s) in charge of the processing. 3. A data subject shall have the right to obtain a) updating, rectification or, where interested therein, integration of the data; b) erasure, anonymization or blocking of data that have been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed; c) certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected. 4. A data subject shall have the right to object, in whole or in part, a) on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection; b) to the processing of personal data concerning him/her, where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys. **Section 8** *(Exercise of Rights)* 1. The rights referred to in Section 7 may be exercised by making a request to the data controller or processor without formalities, also by the agency of a person in charge of the processing. A suitable response shall be provided to said request without delay. […] 4. Exercise of the rights referred to in Section 7 may be permitted with regard to

	data of non-objective character on condition that it does not concern rectification of or additions to personal evaluation data in connection with judgments, opinions and other types of subjective assessment, or else the specification of policies to be implemented or decision-making activities by the data controller.
Article 16: Confidentiality	**Section 26** *(Safeguards Applying to Sensitive Data)* […] 5. Data disclosing health may not be disseminated. **Section 30** *(Persons in Charge of the Processing)* 1. Processing operations may only be performed by persons in charge of the processing that act under the direct authority of either the data controller or the data processor by complying with the instructions received. 2. The aforementioned persons shall be nominated in writing by specifically referring to the scope of the processing operations that are permitted. This requirement shall be also fulfilled if a natural person is entrusted with the task of directing a department, on a documentary basis, whereby the scope of the processing operations that may be performed by the staff working in said department has been specified in writing.
Article 17: security of data processing	**Section 17** *(Processing Operations Carrying Specific Risks)* 1. Processing of data other than sensitive and judicial data shall be allowed in accordance with such measures and precautions as are laid down to safeguard data subjects, if the processing is likely to present specific risks to data subjects' fundamental rights and freedoms and dignity on account of the nature of the data, the arrangements applying to the processing or the effects the latter may produce. 2. The measures and precautions referred to in paragraph 1 shall be laid down by the Garante on the basis of the principles set out in this Code within the framework of a check to be performed prior to start of the processing as also related to specific categories of data controller or processing, following the request, if any, submitted by the data controller. **Section 31** *(Security Requirements)* 1. Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimize, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected. **Section 34** *(Processing by Electronic Means)* 1. Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B: a) computerised authentication, b) implementation of authentication credentials management procedures, c) use of an authorisation system, d) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenancing electronic means, e) protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software, f) implementation of procedures for safekeeping backup copies and restoring data and system availability, g) keeping an up-to-date security policy document [Repealed by Section 45(1)c. of decree 5/2012 as subsequently converted, with amendments, into Act no. 35 dated 4 April 2012.]

	TECHNICAL SPECIFICATIONS CONCERNING MINIMUM SECURITY MEASURES (ANNEX B) PROCESSING BY ELECTRONIC MEANS The following technical arrangements shall be implemented by the data controller, data processor – if appointed – and person(s) in charge of the processing whenever data are processed by electronic means: ***Computerised Authentication System*** 1. Persons in charge of the processing shall be allowed to process personal data by electronic means if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations. 2. Authentication credentials shall consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password. 3. One or more authentication credentials shall be assigned to or associated with each person in charge of the processing. 4. The instructions provided to the persons in charge of the processing shall lay down the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care. 5. Where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive or judicial data are processed, the password shall be modified at least every three months. 6. An ID code, if used, may not be assigned to another person in charge of the processing even at a different time. 7. Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management purposes. 8. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data. 9. The persons in charge of the processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions. 10. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the processing, without delay, as to the activities carried out. 11. The provisions concerning the authentication system referred to above as well as those concerning the authorisation system shall not apply to the processing of personal data that are intended for dissemination.

	Authorisation System 12. Where authorisation profiles with different scope have been set out for the persons in charge of the processing, an authorisation system shall be used. 13. Authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to start of the processing in such a way as to only enable access to the data that are necessary to perform processing operations. 14. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply. ***Other Security Measures*** 15. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile. 16. Personal data shall be protected against the risk of intrusion and the effects of programmes as per Section 615-quinquies of the Criminal Code by implementing suitable electronic means to be updated at least every six months. 17. The regular update of computer programmes as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually. If sensitive or judicial data are processed, such update shall be carried out at least every six months. 18. Organisational and technical instructions shall be issued such as to require at least weekly data back-ups. ***Security Policy Document*** 19. [Repealed] […] ***Additional Measures Applying to Processing of Sensitive or Judicial Data*** 20. Sensitive or judicial data shall be protected against unauthorised access as per Section 615-ter of the Criminal Code by implementing suitable electronic means. 21. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and processing. 22. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means. 23. If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days. […]
Article 21: processing operations must be publicized	**Section 25** *(Bans on Communication and Dissemination)* 1. Communication and dissemination shall be prohibited if an order to this effect has been issued by either the Garante or judicial authorities, as well as a) with regard to personal data that must be erased by order, or else upon expiry of the term referred to in Section 11(1), letter e), b) for purposes other than those specified in the notification, whenever the latter is to be submitted. […]
Not specified in this declaration.	**Section 28** *(Data Controller)* 1. Whenever processing operations are carried out by a legal person, a public administrative agency or any other body, association or organisation, the data

	controller shall be either the entity as a whole or the department or peripheral unit having fully autonomous decision-making powers in respect of purposes and mechanisms of said processing operations as also related to security matters.

In addition, the Personal Data Protection Code includes a guideline regulating the compensation of harm, caused by the project team.

Section 15 *(Damage Caused on Account of the Processing)*

1. Whoever causes damage to another as a consequence of the processing of personal data shall be liable to pay damages pursuant to Section 2050 of the Civil Code.

2. Compensation for non-pecuniary damage shall be also due upon infringement of Section 1.

(Italian Data Protection Authority, 2004)

2.3 Other ethical guidelines for research with human participants

In addition to national and international regulations, for the general ethical rules in the Trans.Safe project, ethical requirements of the stakeholders and recommendations of the UNESCO and the World Medical Association will also taken into account.

2.3.1 Ethical Requirements of Trans.Safe Stakeholders

Regarding the collecting of individual data of **VAG employees**, the VAG human resources department demands the observance of the following principles:

- No data can be collected through interventions on the human body:
  - No blood samples can be taken,
  - no field sobriety test can be taken,
  - no hair-sample can be taken.
  - Data collection has to be based on voluntariness.
- Data collection has to be anonymous.
- Data should not be made public.
- It is not allowed to evaluate the data in order to check the performance of the staff.
- In case of a commercial product, the data must not be stored.
- During the project phase it is allowed to store and to verify the data against observation or video data.
- The persons should be able to work freely without any cabling.

(VAG Human resources department 2014)

2.3.2 Declaration of Helsinki

One aim of the Trans.Safe project is to measure and monitor stress parameters. Different to common stress measurement and monitoring procedures, ambient body-worn sensors will be used to detect stress in this project, assuring unobtrusive physiological measurement (for further details see Trans.Safe 2013, p.9). However, even with unobtrusive measurement, the processing of physiological data is an especially sensitive topic.

To ensure the integrity and dignity of the data subject, the following guidelines of the “Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects” of the World Medical Association (WMA) will be taken into account whenever physiological data of participants is processed. The declaration is mainly addressed towards physicians, but will be rendered and abridged, appropriate for the special challenges of the Trans.Safe project.

- […]

- It is the duty of the physician to promote and safeguard the health, well-being and rights of patients, including those who are involved in medical research. The physician's knowledge and conscience are dedicated to the fulfillment of this duty.
- […]
- Medical research is subject to ethical standards that promote and ensure respect for human subjects and protect their health and rights.
- While the primary purpose of medical research is to generate new knowledge, this goal can never take precedence over the rights and interests of individual research subjects.
- It is the duty of physicians who are involved in medical research to protect the life, health, dignity, integrity, right to self-determination, privacy, and confidentiality of personal information of research subjects. […]
- Physicians must consider the ethical, legal and regulatory norms and standards for research involving human subjects in their own countries as well as applicable international norms and standards. […]
- […]
- Medical research involving human subjects must be conducted only by individuals with the appropriate ethics and scientific education, training and qualifications. […]
- […]
- Appropriate compensation and treatment for subjects who are harmed as a result of participating in research must be ensured.
- […]
- Medical research involving human subjects may only be conducted if the importance of the objective outweighs the risks and burdens to the research subjects.
- All medical research involving human subjects must be preceded by careful assessment of predictable risks and burdens in comparison with foreseeable benefits […].
- Measures to minimize the risks must be implemented. […]
- […]
- When the risks are found to outweigh the potential benefits or when there is conclusive proof of definitive outcomes, it must be assessed whether to continue, modify or immediately stop the study.
- […]
- Medical research involving human subjects must conform to generally accepted scientific principles, be based on a thorough knowledge of the scientific literature, other relevant sources of information […].
- The design and performance of each research study involving human subjects must be clearly described and justified in a research protocol.
- The protocol should contain a statement of the ethical considerations involved and should indicate how the principles in this Declaration have been addressed. […]
- […]
- Every precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information.
- Participation by individuals, capable of giving informed consent, must be voluntary […], preferably in writing. […]
- […]
- […] Researchers have a duty, to make publicly available the results of their research on human subjects and are accountable for the completeness and accuracy of their reports. All parties should adhere to accepted guidelines for ethical reporting. Negative and inconclusive as well as positive results must be published or otherwise made publicly available. […]

(WMA 2013)

2.3.3 UNESCO MOST

In 1994, the UNESCO established the project “MOST” (Management of Social Transformations) “[…] to promote policy-relevant social science research […]”. Within this project, ethical guidelines were defined, to “[…] draw the attention of all researchers to certain areas in which conflicts between ethical principles and aims of the research might arise, and to stress the need for their resolution.”

According to MOST, the following 19 guidelines must be observed in every social science research project:

1 Responsibility for all procedures and ethical issues related to the project rests with the principal investigators.
2 Research should be conducted in such a way that the integrity of the research enterprise is maintained, and negative after-effects, which might diminish the potential for future research, should be avoided.
3 The choice of research issues should be based on the best scientific judgement and on an assessment of the potential benefit to the participants and society in relation to the risk to be borne by the participants. Studies should relate to an important intellectual issue.
4 The researcher should consider the effects of his/her work, including the consequences or misuse, both for the individuals and groups among whom they do their fieldwork, and for their colleagues and for the wider society.
5 The researcher should be aware of any potential harmful effects; in such circumstances, the chosen method should be used only if no alternative methods can be found after consultation with colleagues and other experts. Full justification for the method chosen should be given.
6 The research should be conducted in a competent fashion, as an objective scientific project and without bias. All research personnel should be qualified to use all of the procedures employed by them.
7 The research should be carried out in full compliance with, and awareness of, local customs, standards, laws and regulations.
8 All researchers should be familiar with, and respect, the host culture. Researchers undertaking research on cultures, countries and ethnic groups other than their own should make their research objectives particularly clear and remain aware of the concerns and welfare of the individuals or communities to be studied.
9 The principal investigators' own ethical principles should be made clear to all those involved in the research to allow informed collaboration with other researchers. Potential conflicts should be resolved before the research begins.
10 The research should avoid undue intrusion into the lives of the individuals or communities they study. The welfare of the informants should have the highest priority; their dignity, privacy and interests should be protected at all times.
11 Freely given informed consent should be obtained from all human subjects. Potential participants should be informed, in a manner and in language they can understand, of the context, purpose, nature, methods, procedures, and sponsors of the research. Research teams should be identified and contactable during and after the research activity.
12 There should be no coercion. Participants should be fully informed of their right to refuse, and to withdraw at any time during the research.
13 Potential participants should be protected against any and all potentially harmful effects and should be informed of any potential consequences of their participation.
14 Full confidentiality of all information and the anonymity of participants should be maintained. Participants should be informed of any potential limitations to the confidentiality of any information supplied. Procedures should be put in place to protect the confidentiality of information and the anonymity of the participants in all research materials.
15 Participants should be offered access to research results, presented in a manner and language they can understand.
16 All research should be reported widely, with objectivity and integrity.

17 Researchers should provide adequate information in all publications and to colleagues to permit their methods and findings to be properly assessed. Limits of reliability and applicability should be made clear.

18 Researchers are responsible for properly acknowledging the unpublished as well as published work of other scholars.

19 All research materials should be preserved in a manner that respects the agreements made with participants.

(UNESCO MOST 2003)

2.4 Ethical principals in the Trans.Safe project

For a better understanding of the implementation of the stated ethical guidelines into the daily work of the project members, the main aspects of the aforementioned regulations will be illustrated in a more tangible manner in the following sections.

2.4.1 Consent, full information and the rights of the data subject

***Informed consent** of the data subjects, ensuring their voluntary participation in the project, is a necessary condition for the processing of the subjects data.*

Informed consent of all data-subjects participating in the project will be ensured through **full information** about the goals of the study and about the type of data being recorded through interviews, observation and/or testing of prototypes the data-subjects are participating in. This consent will be captured in written form.

The informed-consent form used is based on the recommendations of the "Ambient assisted living joint Program"[1]. The form contains the following aspects:

- A description of the project and its aims – accessible with respect to language and content
- A specification of the role(s) of different data-subjects and end-users in the project
- For the prototype-testing: information about their self-determination (data-subjects and end-users must be able to turn off systems or services at their own discretion)
- Information about the compensation provided to the primary data-subjects (expenses or fees paid, etc.)
- Information about the contact person in the project (for ethical issues and related questions)
- Information about the exit rights for individual data-subjects (information about the procedure for withdrawal from the project at any time, without giving a reason and without incurring costs or penalties)

(cf. AALA CMU 2013, p.21)

To meet all legislative requirements, the form also contains the following additional aspects:

- Information about the identity of the controller processing the data
- Information about the categories of recipients of the collected data
- Information about the modalities of collection, progressing and storing of the data
- Information about the free choice of the data subject to provide data or not to
- Information about the right of access to and correction, erasure and blocking of the personal data, if necessary or desired (only possible, as long as the database, storing the identifying characteristics, exists – see chapter 2.4.3). This right although includes the right of information about personal data being stored, and the source of this data.

[1] The „Ambient assisted living joint Programm" is a union of AAL partner-states, financially supported by the European Commission.

- For the collection of physiological (stress) data: explicit information about the collection and processing of this sensitive data

The consent is to be obtained prior data-collection. The data subject will be specifically indicated to this form.

*The **right of access of the data subjects** to their personal data, processed and stored, will be obtained.*

If a data subject desires to exercise his or her right of access to his or her data, this request will be forwarded to the project-member concerned, no matter whom of the Trans.Safe team the data subject approaches for this matter.

The data subjects will then receive information about their right of access to, and correction of their personal data, if necessary. Enquiries (no formalities necessary) of the data subjects will be handled as quickly as possible. If the data subject objects, his or her data will be deleted, even though they are relevant to the purpose of the collection.

2.4.2 Fair and lawful processing, purpose and data quality

*The data subjects **privacy and dignity** must be respected and protected by all project members and must not be jeopardized by inappropriate methods.*

To be able to analyze the routines of the data subjects via the shadowing-technique[2] and for (personal) interviews and enquiries with the participants in the field tests, the interviewers and examiners may arrange to meet at the data-subjects workspace. The interviewers will be instructed to always obtain permission to visit in advance and to respect the persons' **privacy and dignity** in all circumstances.

*Personal data must only be collected and processed for a **specific, explicit and legitimate purpose**.*

For the Trans.Safe project, personal data will solely be processed for the ultimate, legitimate and ex ante-defined goal of developing a system, supporting senior workers who can and wish to stay actively longer in a job position with high personal and public safety risks. For this purpose a technical solution will be developed, serving three aims:

- Stress parameter (overwork/under-challenge) measurement and real-time information
- Ambient stress response
- Evaluation, encouragement and work flow adaption.

(For further details of the purposes of the Trans.Safe project see: Trans.Safe 2013)

*The data processed, and the methods and technological devices used must be in **proportion** and therefor **adequate, relevant and not excessive** in relation to the purpose of the Trans.Safe project.*

As already stated above, in the observation phase the data-subjects **won't be hindered in their freedom** at work. Therefor, the data subjects won't be cabled.

Furthermore, no data will be evaluated in order to check the performance of staff and no data will be collected through interventions on the human body:

- No blood samples will be taken
- No field sobriety test will be taken
- No hair-sample will be taken

[2] The shadowing-technique is an observation method for the collection of information about a person's everyday activities and natural environment through visits and accompaniment of users in their natural environment. (cf. youse 2013)

Furthermore, only the **minimum number of data** will be collected, that is necessary to be able to validate the algorithms of the technological solution developed in the project. In addition, the device (especially necessary sensors), even in its prototype-phase, will be adequate to its purpose, will only collect minimal data and won't hinder the test- and end-users at their work. Since the finished device will be based on ambient-, minimal invasive sensors, -monitoring the environment and movement, beside physiological factors- the device won't be intrusive.

As soon as possible, data will be **pseudonymised**[3] and identifying data will be deleted (see chapter 2.4.3) The pseudonymised data will be kept, beyond the Trans.Safe project, for scientific purposes. Further processing, independent of the Trans-Safe project, must not be inconsistent with the original purpose of the data collection, processing and storage.

The **accuracy of the processed personal data** will be ensured by thorough collection, recording and analysis of data. Errors appearing, despite the careful processing of data, will be adjusted or - if necessary - deleted, and the adjustment will be immediately communicated to all project-members, involved in the processing of data.

*For the lawful processing of data, **customs, standards, laws and regulations** of the concerned states, companies and institutions will be considered and observed.*

Therefore, European, German and Italian legislations were consulted and ethical recommendations of influential institutions were studied. Additionally, general requirements for the end-device, of affected data-subjects, test- and potential end-users and their employers, will be determined through interviews.

2.4.3 Confidentiality, anonymity and data protection

*In the Trans.Safe project, **confidentiality** plays an especially important role, since highly sensitive data – physiological stress-parameters and general data allowing conclusions about the performance of employees at their work - are processed.*

*The **confidentiality** of captured personal data (such as age, gender, state of health status) will be assured.*

Confidentiality of personal data will be achieved, whilst data can only be collected, processed and used by persons employed in data processing, if authorization is granted. The persons involved in the data processing are required to give an undertaking to maintain confidentiality, which continues to be valid, even after the termination of their occupation. The processing operations will be specified in writing and this document will serve as instruction for the data processors.

*The anonymity of the subjects will be achieved through **pseudonymisation**. The German Federal Data Protection Act defines this "Aliasing" as the replacement of the data-subjects name and other identifying characteristics with a label to disguise this data or make the identification of the subject substantially difficult. (juris 2013, art.3/6a)*

Therefore, data will be stored in two separate databases. One with the identifying characteristics, such as name, address and the label - the other database with the remaining data. During the project phase, personal data is stored to verify the data against observation or video data. As soon as possible, the first databank will be deleted and the content of the second database will be anonymised.[4]

The pseudonymised data will be kept, beyond the Trans.Safe project, for scientific purposes (see chapter 2.4.2).

*As stated in the directive 95/46/EC, appropriate **technical and organizational data protection measures** must be taken, to prevent the destruction or loss, alteration or unauthorized disclosure*

[3] Pseudonymization takes the most identifying fields within a database and replaces them with one or more artificial identifiers, or pseudonyms (e.g. a name is replaced with a unique number).

[4] The German Federal Data Protection Act defines anonymization as "modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labor be attributed to an identified or identifiable individual." (juris 2013, §3 art. 6)

or access to personal data when it is processed, stored or transmitted.

The data security and protection will be assured through the following organizational and technical measures:

Organizational:

- The raw data gathered cannot leave the closed loop system and are only accessible within the closed loop. Only abstracted data will leave the local system: Data will be transferred from one partner to another within the consortium only after made anonymous.
- The data subjects will be informed about their rights with regard to data protection and privacy.
- The database containing identifying characteristics will be deleted as soon as possible.
- Data can only be processed in accordance with the instructions of the principal.
- Persons employed in data processing are introduced to leave no technology unattended.

Technical:

- All data (pseudonymised) is stored on a secure server of the Hochschule Luzern (HSL)
- Through the platform 'Confluence', data can be added, altered or deleted solely by authorized project members.
- The platform allows determining whether and by whom personal data have been added to, or altered on the platform.
- Personal data cannot be accessed without it being noticed by the institution responsible for the protection of the data and legitimate other partners of the consortium.
- The 'Confluence' server is secured through a password with more than eight characters and without relation to the processor in charge. This password is only disposed to authorized project members. Every authorized person has an individual password, making it possible to restrict the access to data to a certain group of people.
- In regular intervals, this password is alternated.
- The system can be reset to its default setting at any time, thus enabling a test person to obliterate his or her personal data if he or she so wishes.
- Procedures for safekeeping: backup copies (at least every week)?
- Security policy document?
- Regular update of computer program? (at least annually – sensitive data: every 6 months)

2.4.4 Scientific Standards and Publication

*The processing of data must follow general **scientific principles,** must be based on a broad knowledge of significant **scientific literature** and studies and must be objective. This ensures high quality of data, the general results and the end-device. (Validity, reliability, objectivity)*

For the stress measurement in the Tans.Safe project, **validity**[5] of the used research instruments is very important. To assure the valid measurement of stress, it has to be defined, how, and through which indicators, the concept of stress can be measured. Therefore, an appropriate theoretical concept, including insights from scientific literature and studies, must be developed. Possible interfering indicators must be anticipated, respectively recognized.

To assure **reliable**[6] research results, measures must be used, which would, if repeated, produce the same results. To produce such stabile results, standardised measures are applied in this project. For the qualitative interviews and the shadowing technique, structured interview-guidelines and standardised observation-protocols are used.

(For more information to validity and reliability, see: Field 2009, pp.11)

[5] „Validity refers to wether an instrument measures what it was designed to measure." (Field 2009, p.11)

[6] " […] reliability, which is the ability of the measure to produce the same results under the same conditions." (ibid. p.12)

This standardisation contributes to the **objectivity** of the researchers. Also, in advance to the project and regularly during the project, the consortium collects expectations and existing preconceptions of every researcher involved, to achieve awareness and reflection.

The **research design is documented** in detail in. The practical approach is described in a research protocol. This deliverable is part of this research protocol, describing the implementation of the set ethical and legislative principles in research practice.

*The processing of data must only be conducted by **qualified and trained researchers**.*

All members of the project consortium possess broad experiences in the exploration and development of innovations in the AAL-sector. (For a detailed overview of the qualities of the project members and their staff, see Trans.Safe 2013, pp. 21)

*The **dissemination and publication** of the results obtained, are one of the primary aims of scientific researchers. The publication of the results involves the conflict between privacy interests of the individual participant and the need for free exchange between scientific experts. The report of the results must be complete and accurate.*

A detailed description of the results, used methods and limits of the research will be **published** after the projects completion. For statistical analysis only data, which are made anonymous, are used and results -especially concerning health data- are only published as summary statistics to prevent re-identification of individual subjects. For public use of media, created during user trials and workshops, an informed consent from will be used. Negative as well as positive results will be made publicly available and the limits of reliability and applicability will be made clear. This Deliverable is a first report of the methods and arrangements for the compliance of legal and ethical principals.

2.4.5 Further ethical principals

*The **ethical principles of all project-members** must be transparent, to allow informed collaboration.*

At the beginning of the Trans.Safe project the consortium defined its intern ethical guidelines. During the analysis phase, all stakeholders were questioned about their ethical principals and important requirements, which must be considered for the development of the end-device. This deliverable summarizes the important ethical principals of all involved parties and enables a consistent ethical approach of all project members in all phases of Trans.Safe.

***Benefits and risks** – Research can only be conducted and new technologies and services can only be tested, if the benefits outweigh the risks. Risks taken must be in relation to possible benefits of the study and furthermore must be minimized. The study should benefit the participants and the society.*

The end-device resulting of the Trans.Safe project, is expected to improve the quality of life for end-users (older employees and employees in general) and to bring benefits for the project-partners, but although for employers and the society in general. The solution is expected to:

- Increase health by reducing stress at the working place
- Increase security at the work place
- Improving employability for older employees
- Using competence and experience of older employees

(For further details see Trans.Safe 2013, pp. 32)

Possible/ Predictable risks of research methods or the end-device?

- leakage of personal data
- *usage of stress-data in order to check the performance of the staff*

*The **harm** of data-subjects and end-users must be **avoided** under any circumstances, especially regarding technical devices and services potentially developed and tested in this project. The collection of data and developed technologies or services cannot damage the dignity and integrity of the data-subjects and end-users.*

To prevent harm in the analysis phase, due to the leakage of personal data, the above mentioned organizational and technical measures are taken.

To avoid harm of the test- and end-user, as already mentioned, stress-parameters are only measured with non-invasive procedures. To prevent the risk of illegitimate evaluation of stress-data, in the test-phase only authorized Trans.Safe members are able to access those data.

The end-device must ensure the confidentiality of collected stress-data. Potential evaluation-

*If harm of the participant is caused, by project-members or the study in general, **compensation must be granted.***

features disclosing stress-data, will only be accessible for the end-user.

***Well-being of the data-subject** - All measures data-subjects and end-users are involved in must be done for their benefit.*

IMPLEMENTATION?

The outcome of Trans.Safe is supposed to benefit older employees at a stressful working place. Only data-subjects and users are involved which are expected to benefit of the achievements of this project. Hence it was laid down in the “Description of Work” of the Trans.Safe project, that: “users and employers who/which so wish will be granted the right to keep the products they have been provided with for testing and evaluation. No end user involved in the project will lose the opportunity of the continued use of any product that has contributed to an improved quality of life for the single individual, as the end users have contributed to the result of the project.” (Trans.Safe 2013, p. 13)

2.5 General ethical guidelines for the Trans.Safe project team

Based on national and international regulations, the recommendations of experienced institutions and organizations and the ethical principals and organizational requirements of the project-members, the project-team has set the following general rules, mandatory in every phase of the Trans.Safe project where data will be processed:

- ✓ **Informed consent -** The data collection and prototype testing is based on voluntariness and full information of the data-subjects and users and is documented in written form.
- ✓ **Self-determination -** Data-subjects and users have the right to withdraw from the research-program at any time and without any consequences. The participants have to be fully informed about this right.
- ✓ **Privacy and dignity -** The data subjects privacy and dignity must be respected and protected by all project members and must not be jeopardized by inappropriate methods.
- ✓ **Purpose specification and quality of data -** Personal data must only be collected and processed for a specific, explicit and legitimate purpose, identified before the collection and processing of data. Every reasonable step must be taken to ensure that inaccurate or incomplete data is erased or rectified.
- ✓ **Proportion and Relevance -** The data processed and the methods and technological devices used, must be in proportion and therefor adequate, relevant and not excessive in relation to the purpose of the specified goal of the study project. Only the minimum number of data required for a certain purpose must be collected. No data will be used to evaluate the performance of the data-subjects.

- ✓ **Confidentiality and Anonymity -** The Data collection is anonymous. Confidentiality of all collected data and the anonymity of the data-subjects must be assured. Personal Data won't be made public.
- ✓ **Right of access -** The right of access of the data subjects to their personal data, processed and stored, will be obtained.
- ✓ **Compliance and adaption -** Customs, standards, laws and regulations of the concerned states, companies and institutions will be considered and observed.
- ✓ **Security measures and data storage -** Appropriate technical and organizational data protection measures must be taken, to prevent the destruction or loss, alteration or unauthorized disclosure or access to personal data when it is processed, stored or transmitted.
- ✓ **Scientific standards -** The processing of data must follow general scientific principles (validity, reliability), must be based on a broad knowledge of significant scientific literature and studies and must be objective.
- ✓ **Qualifications of persons employed in data processing -** The processing of data must only be conducted by qualified and trained researchers.
- ✓ **Publication -** A detailed description of the results, used methods and limits of the research will be published after the projects completion.
- ✓ **Disclosure of the ethical principals of the consortium -** The ethical principles of all project-members must be transparent, to allow informed collaboration.
- ✓ **Benefits and risks -** Research can only be conducted and new technologies and services can only be tested, if the benefits outweigh the risks. Risks taken must be in relation to possible benefits of the study.
- ✓ **Avoiding Harm -** The harm of data-subjects and end-users must be avoided under any circumstances; the dignity and integrity of the data-subjects and end-users must not be damaged.
- ✓ **Compensation of Harm -** If harm of the participant is caused, by project-members or the study in general, compensation must be granted.
- ✓ **Well-being of the data-subject** - All measures data-subjects and test- and end-users are involved in, must be done for their benefit.

3 Legal considerations

3.1 Introduction

"Every driver shall at all times be able to control his vehicle […]" (art. 8 par. 5),

states the Convention on Road Traffic, held 1968 in Vienna, and then later

*"Every driver of a vehicle shall in all circumstances have his vehicle under control so as to be able to exercise due and proper care and to be at all times in a position to perform all manoeuvres required of him" (*art. 13 par. 1 p. 1).

Regarding questions of liability, the world was rather simple in 1968 with a clear allocation of roles. The driver was held responsible for behavioral aspects as well as actions related to driving while the car manufacturers were accountable for supplying proper and safe materiel, i. e. vehicles. The jurisdiction of behavioral aspects thus is generally specified by national road traffic regulations to which the driver has to obey (regulatory laws). In contrast, manufacturers are required to comply with approval regulations as well as product liability laws (tort law).

The technological advancements of the last decades have enabled the development of sophisticated in-vehicle information systems (IVIS) and advanced driver assistance systems (ADAS). On the one hand, such systems hold the potential to support the driver and thus increase driving comfort and traffic safety (e. g., Kühn & Hannawald 2015). On the other hand, not only the number of systems interacting with the driver at the same time is on the rise. In addition, ADAS apply functions cutting deeper and deeper into the primary task of driving. Thus, they take-over more and more tasks and functionalities for which the driver was hold responsible in the past.

This raises questions about who is responsible in case of a traffic offences or traffic accidents. Can the driver still be hold accountable or should manufacturers increasingly bear responsibility? As indicated by the two opening citations, the term "control" is a key aspect regarding such reflections. The question who, i. e. the driver or the system, has been in charge of controlling the vehicle might therefore very well be the bone of contention in many legal disputes. To shine a light on the current legal state, we first take a look at the current driver image from a legal point of view. Thereafter, we split up the topic into two branches. First, we analyze *controllability* and its implication within regulatory laws. Secondly, we do the same in the context of liability laws. After introducing the meaning of the two legal concepts, we elaborate its importance in the context of guidelines, directives, and standards such as RESPONSE 3's Code of Practice (CoP), ISO 26262 and the European Statement of Principles on Human Machine Interface (ESoP).

3.2 Driver image in legal contexts

In traffic law – rarely presented in the relevant case-law, but often used in legal provisions – there are many terms related directly to the driver, like **"optimal driver"**, **"moment of shock"**, **"error in the heat of the moment"**.

In view of the requirements concerning *controllability* it is important to consider these terms as well. However, it has to be scrutinized whether these terms are still appropriate in light of automated functionalities and ADAS.

„Optimal driver"

According to § 17 Abs. 3 StVG (German road traffic law) liability of vehicle owner does not apply if an accident is caused due to an inescapable event. In § 17 Abs. 3 S. 2 StVG an inescapable event is defined as an event which cannot be prevented by highly carefulness including appropriate and quick-thinking acting of the driver in coherence of all potential danger. In appraising events it is more important if an ideal driver would have maneuvered himself into the danger situation than how he would have reacted.

As an inescapable event in legal interpretation is a "friendly green traffic light", when a motorcyclist falls right bevor overtaking or a car is being flanged into the oncoming traffic lane. As an escapable event in legal interpretation on the other side is when a car is send into skid on a

recognizable wet and slippery road, when a car which is parked in a no parking zone covers the view on the traffic for another car and causes this way an accident. It is important that the question of an inescapable event and the optimal driver always considers particular circumstances each individual case.

In respective of the controllability of such systems, which take over driving tasks, it is most likely that the requirements for the optimal driver for technical systems will be at least on the same or even higher level than the requirements for the optimal driver for human beings. Provably mistakes in construction, concept or instruction in controllability of the system will be seen in legal interpretation as a fault of the consistency of the vehicle and not as an inescapable event. Faults of the consistency of the vehicle are for example: mistakes in construction, caring out the constructions or poor maintaining, such as fails of regulation of cruise control, adaptive cruise control or even interior components if they handicap the road safety. (Berz & Burmann, 2012, Kap. 4 A, Rdnr. 50).

„Moment of shock“

In case of unpredictibale hazards, the so-called moment of shock is awarded also to the optimal driver (Berz & Burmann, 2012 Kap. 4 A, Rdnr. 47). In contrast to the reaction time, which has to be considered permanently, the so-called shock time can be awarded to the driver additionally under certain circumstances. For example, this could be an abrupt malfunction of the service brake or a bursting tyre, which surprise the driver in an unexpected way.

***„Human* error“**

Furthermore, the jurisdiction knows the term „human error“ regarding the human in his role as driver. In coherence with the level of culpability (ordinary or culpable negligence), the human error plays an important legal role.

As a matter of course, the mentioned terms are a privileging of human drivers, which has no equivalent for non-conforming, automated interventions of a function.

3.3 Controllability and regulatory law

Legally, the two citations from the Vienna Convention on Road Traffic in the introduction above ask for regulatory requirements and would as such be classified as regulatory law. However, from a juridical point of view the Convention on Road Traffic makes up for an international treaty. Therefore, it has no means to require the citizens of any country to obey to these regulations directly. Instead the signing countries are in charge to create or change national laws in such a manner as to be in accordance with the resolution of the convention.

In Germany, the corresponding requirements are incorporated in the form of numerous regulations within the so called *Straßenverkehrs-Ordnung* (StVO; corresponds approximately to traffic or highway code in Anglo-American countries). First and foremost, the regulatory order of § 1 Abs. 1 StVO is the fundament for all later, more specific regulations. It requires “permanent care and mutual respect” (own translation) from all traffic participants. Examples of more specific regulations are:

- § 3 Abs. 1 StVO, which regulates i. a. that a driver may operate her vehicle only up to a speed for which she is at all times able to control her machine.
- § 4 StVO deals with aspects of clearance to preceding vehicles.

Judgments with regard to these regulations of the StVO in Germany presume a conception of human being.

“Traffic participant is the one who acts […] physically and directly – trough action or in breach of one's duty – on the progress of traffic events”.

A function in the sense of a *“general clause”* is attributed to § 1 which allows the "continuing education" of the traffic regulations to “the ever-changing technical conditions” (vgl. Burmann et al., 2012, § 1 StVO, Rdnr. 3). This emphasizes that the regulatory law requires the driver to “control” the vehicle she is operating.

3.4 Controllability and liability law

The controllability has an important relevance not only for the above-noted regulatory law, but also for product liability laws. In § 3, passage 1, the product liability law (ProdHaftG) defines closer requirements when a product is so-called non-conforming:

"The product is nonconforming, if it does not offer the safety that could be expected under all circumstances, especially

a. *its performance*
b. *its practice, the user can expect justifiably*
c. *its point in time, it was introduced."*

Therefore, the product has to be conditioned regarding construction, production and instruction in a way, that the physical intactness of the user or of others or someone's private property is not harmed (Palandt, 2013, § 3 ProdHaftG, Rdnr. 2). It has to be developed with respect to the state-of-the-art of science and technology, which are described in technical standards (for example, DIN-norms) and to statutory safety requirements, the generality can expect (Palandt, 2013, § 3 ProdHaftG, Rdnr. 4).

The duty of replacement through the manufacturer is excluded, if a nonconformance could not be recognized although the state-of-the-art of science and technology was considered at that time (§ 1 Abs. 2 Nr. 5 ProdHaftG).

State-of-the-art means the epitome of general knowledge, which is available in science and technology. It is the all-known sum of knowledge and technology (Duisberg & Appt, 2010, S. 215).

Thus, relevant technical standards like DIN or ISO norms and sectoral guidelines (e.g. VDA or VDI) are more and more important for the definition of minimum standards and the liability norm.

The fulfillment of the norms does not meet the requirements in the case, the technical development or the technical knowledge includes more than it is addressed by norms and regulations or when the use of the products leads to risk, which are not covered in the norms (Palandt, 2013, § 3 ProdHaftG, Rdnr.4).

3.5 RESPONSE3 – Code of Practice (CoP)

RESPONSE refers to a series of three subsequent sub-projects co-funded by the European Comission (EC). Starting with RESPONSE 1 in 1998 and being completed by RESPONSE 3 in 2006, the series aimed at establishing best practice and safety guidelines for the development of electronic in-vehicle systems. A particular focus was put on the design and evaluation of advanced driver assistance systems (ADAS) with a major outcome being a corresponding code of practice (CoP): The *"Code of Practice for the Design and Evaluation of ADAS"* [REF]. ADAS are therein defined by the sum of the following features (RESPONSE Consortium 2006, p. 4):

- *"[ADAS] support the driver in the primary driving task*
- *provide active support for lateral and/or longitudinal control with or without warnings*
- *detect and evaluate the vehicle environment*
- *use complex signal processing*
- *direct interaction between the driver and the system".*

Earlier RESPONSE sub-projects emphasize that the guideline's principals shall not be limited to ADAS applications only:

"Other TICS (Transport Information and Control Systems) especially the IVIS (In-Vehicle Information Systems) and cooperative systems (vehicle-to-infrastructure or vehicle-to vehicle communication) may be affected by the principles and rules of the future CoP as well. […] It is explicitly desired to have the enlarged focus also on these non-ADAS systems." (Becker et al. 2004, ???)

3.5.1 Controllability within RESPONSE and RESPONSE 3's code of practice (CoP)

Within the three RESPONSE sub-projects the term *controllability* is not used consistently. In RESPONSE 1 and 2, *controllability* refers to cases of system defects or failures. As such, it indicates the probability to safely deal with such situations and successfully prevent any hazard:

"probability for the success of a manoeuvre, which is intended to counteract a failure and which is executed by a human operator" (Becker et al., 2000, p. 56, RESPONSE 1).

Within RESPONSE 2, its conceptual understanding is directly based on this definition. Furthermore, it comprises drivers' ability to overrule override aspects of However, the focus is moved away from critical situations and onto "ordinary" driving. That is, *"ensuring e. g. permanent overriding possibilities [i. e., in the sense of overruling] and sufficient time frames for driver reaction to guarantee safe take-over manoeuvres from system to driver control"* (Becker et al. 2004, p. 64, RESPONSE 2). In this regard, *controllability* is one of the four fundamental pillars of *safety of use*, next to *comprehensibility*, *predictability*, and *misuse-robustness* (Figure 1).

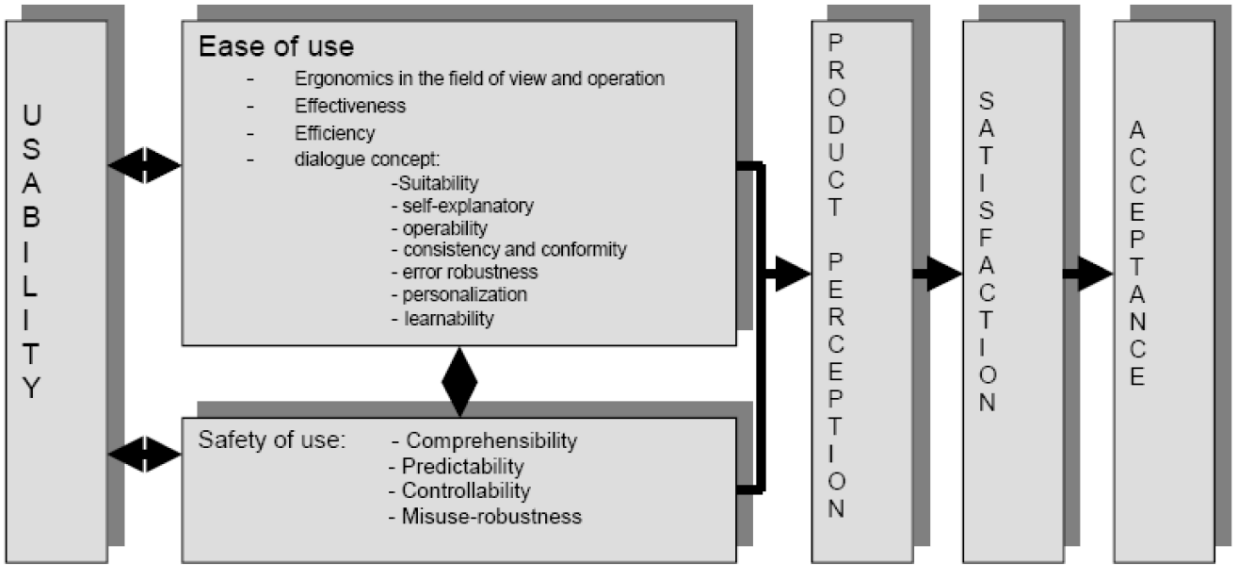

Figure 1: ***Safety of use*** **and its relationship to aspects of usability and user acceptance (Becker et al., 2004)**

Eventually, RESPONSE 3 gives precedence to the concept of *controllability* by defining it within the CoP as the *"likelihood that the driver can cope with driving situations including ADAS-assisted driving, system limits and system failures"* (RESPONSE Consortium, 2006, p.5). Additional explanations suggest however that CoP particularly addresses driver behavior at system boundaries and in case of system malfunctions as well:

"Controllability is dependent on

- *the possibility and driver's capability, to perceive the criticality of a situation,*
- *the drivers capability to decide on appropriate countermeasures (e. g. override, system switch-off) and*
- *the driver's ability to perform the chosen countermeasure (e. g. reaction time, sensory-motor speed, accuracy)."*

Hence, *controllability* aspects of the preceding RESPONSE projects are labeled with the newly introduced term "control issues" in the CoP without being further.

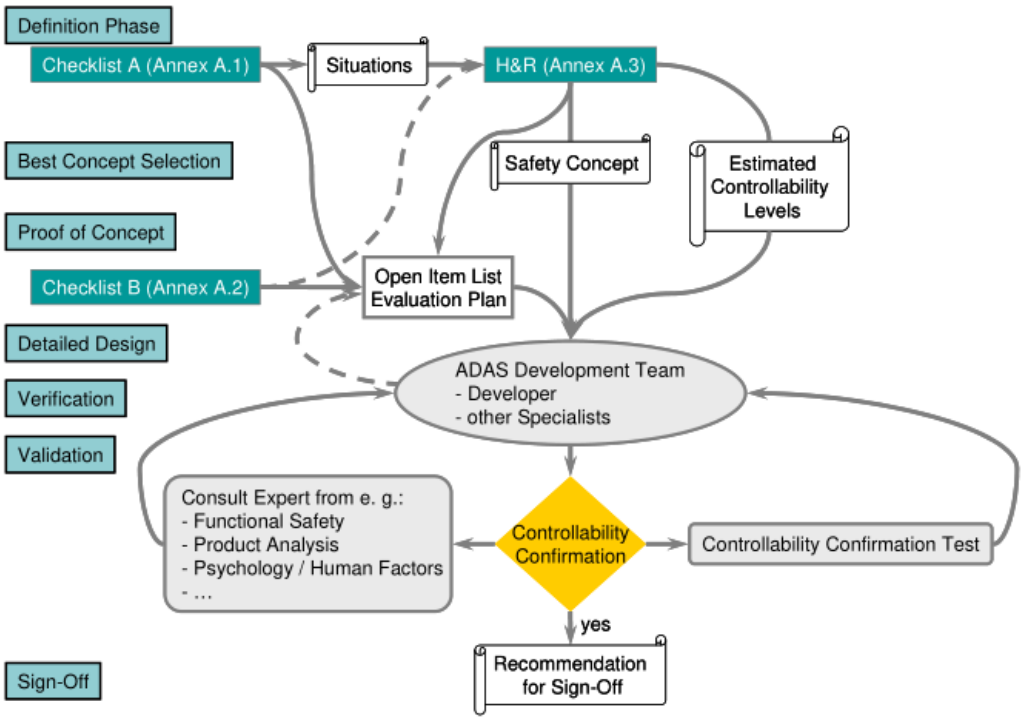

Figure 2: Controllability workflow of the Code of Practice (CoP)

3.5.2 Guidelines for the design and development process

Figure 3 illustrates the proposed design and development process. Since the European Automobile Manufacturers' Association (ACEA) suggested its application in 2009, many vehicle manufacturer and suppliers incorporated these guidelines into their development process.

Key contents of the CoP's guidelines are:

- **Recommendations for the development process:** The concept covers the complete duration starting from the early concept phase up to the completion of the series development. Individual development steps may be performed iteratively. The concept highlights the importance to start elaborating HMI topics as early as during the first steps of the concept phase, i. e. its definition phase. Therefore, the CoP holds specific procedures to perform hazard analyses and risk assessments (see Appendix B). These have to confirm the measures developed with a view to controllability.
- **Comprehensive checklists** supporting these measures: Regarding the design of human machine interfaces, the contents of checklist A and B are of particular relevance. Checklist A is meant to be incorporated during the conception and specification of the assistance system. Checklist B supports the analysis of possible implications of the system. It therefore is part of the ADAS's evaluation.
- **Workflow** for the methodologically **evaluation of controllability (**Figure 2**)**.

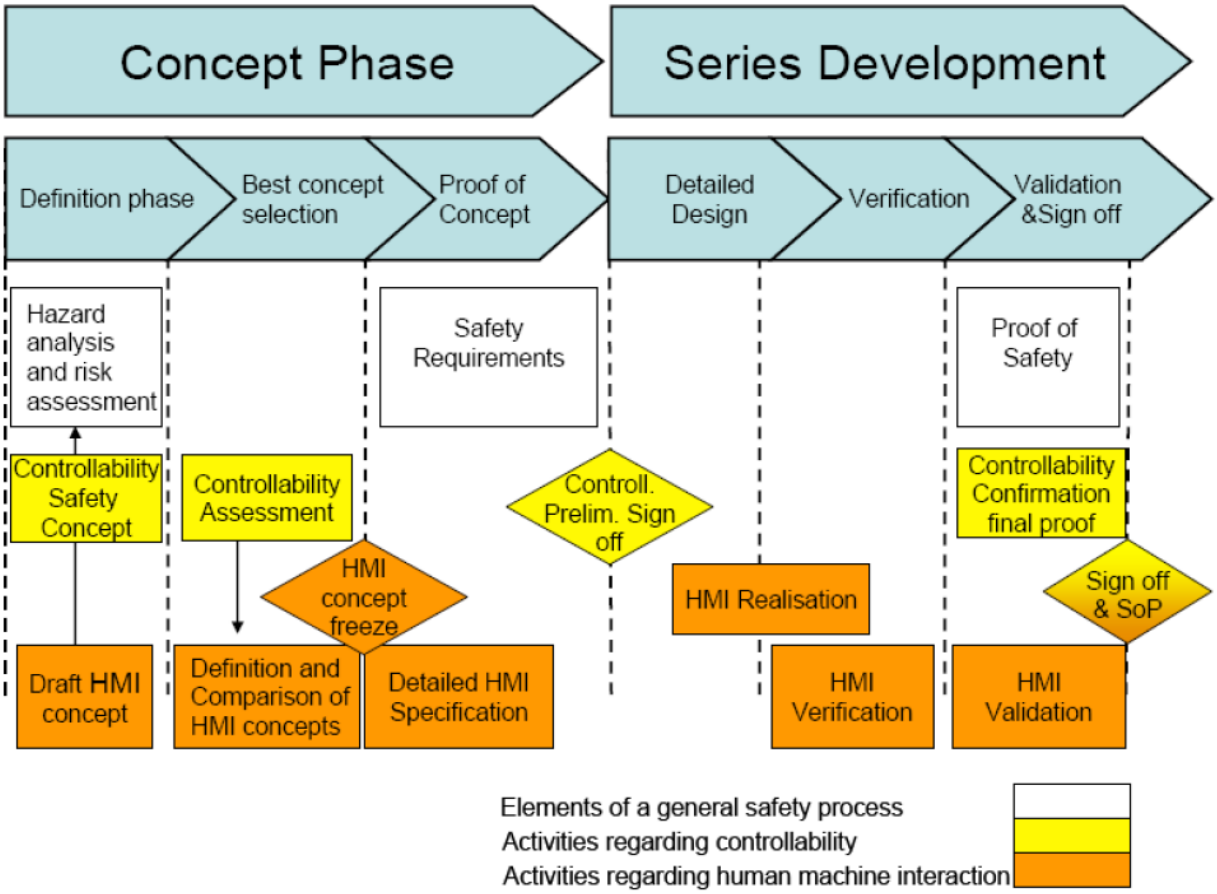

Figure 3: Phases and elements of the ADAS design and evaluation process (RESPONSE Consortium, 2006).

Inhalte der Checkliste A: Spezifikation der Assistenzfunktion

CoP's Checklist A consists of 112 questions regarding different contextual aspects (Table 3). The complete processing of the checklist is recommended as part of the documentation which is necessary for the system's release. The checklist is deployed at distinct parts of the development process's phases – in particular during definition phase (see Appendix B).

Table 3: Overview of the structure and corresponding tables of RESPONSE 3's checklist A

Topics Checklist A / CoP	Detailed Issues
Supported driving task	
	Driving Task Level
	Assistance modes (warning /asisting / interacting)
System Information	
	Functional description
	Situation related limits and sensor limits
	environmental conditions
	dynamic system status in case of system limits
	Infrastructure
	Interaction with vehicles with and without ADAS
	Traffic conditions
HMI and user interaction	
	Direct driver input via ADAS control element
	Non direct driver input via other control elements
	Direct / indirect system feedback
User requirements / User expectations	
	Workload
	User: Requirements / expectations
	Safety aspects of user expectations
	System reliability
System User	
	Intended User Group
	Abilities and restrictions
Preparation of risk analysis	
	hazards
	operation modes
	failure modes
	system limits / detection of system limits
Market	
	Country of operation
Vehicle	
	Vehicle class
	Vehicle type
Homologation / Type approval and	
	Type approval
	General standards
	Technical rules
	State-of-the-art
Functional description	
	Detailed product information
Maintenance	
	Maintenance requirements
	Service

Inhalte der Checkliste B: Evaluation potenzieller Effekte der Systemnutzung

Checklist B deals with potential implications of the assistance system for the driver and road traffic. A first version of the questionnaire was developed within RESPONSE 1 (Kopf et al., 1999). This blueprint contains 60 items, which are assigned to seven contextual categories. These have been cross-classified with 18 so called “evaluation concepts” (Table 4).

The Code of Practice features a revised version of this checklist. In addition to altered formulations of items, the classification into contextual categories and therefore the cross-classification was dropped for the further developed questionnaire. Furthermore, the checklist was extended from 60 to 107 questions.

The classification of the questions was done by means of three properties:

- The items are classified by means of 17 distinct evaluation concepts which correspond to the original concepts to a great extent.
- These evaluation concepts are assigned to different levels of human information processing (Table 5).
- Each item states at which phase of the development process the question should be clarified.

Table 4: Cross-classification of categories and evaluation concepts in RESPONSE 1 (Kopf et al., 1999).

Category	Evaluation concept
Human Machine Interface and System Layout	Perceptibility
System Comprehension	Comprehensibility
Behavioural Aspects	Learnability
Misuse	Predictability
Operability	Controllability
Interaction with Traffic Environment	Behavioural Changes
Economy	Traffic Safety/Risk
	Macroscopic Effects
	Responsibility / Liability
	Driving Efficiency
	Driving Economy
	Workload / Fatigue
	Vigilance
	Error Robustness
	Emotional Issues
	Trust
	Misuse Potential
	Benefits/Acceptance

Table 5: Evaluation concepts and assignment to levels of human information processing within checklist B of RESPONSE 3’s CoP (from Knapp, 2006).

Perception	Decision	Performance
Predictability	Traffic safety / Risk	Misuse potential
Emotional issues	Responsibility / Liability	Macroscopic effects, driving efficiency and economy
Trust	Learnability	Benefits / Acceptance
Perceptibility (message transfer to driver)	Behavioural changes	Operability
Vigilance	Comprehensibility	Control issues

3.6 Meaning of ISO-standard 26262 regarding product liability and controllability

ISO-standards are standardized norms published by the International Organization for Standardization (ISO). Appropriate for this project is Series of standards 26262 ("Road vehicles – Functional safety"), which holds standards for safety related electrical and electronical systems in road vehicles. It obtains for road vehicles up to 3.5 t. Standards adapted to commercial vehicles over 3.5 t and motorcycles are being developed (Winner et.al, 2015, S86). Series of standards 26262 contains process guidelines for the behavior of systems, developing methods including risk analysis of safety related electrical and electronical systems (Duisberg & Appt, 2010, S. 216) and required activities in development and in complete product cycle. *Controllability* is defined in ISO 26262-1.19 as well: "1.19 controllability - ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures".

Therefore, the ISO 26262 defines controllability as the capability to prevent particular danger and damage due to timeous reaction of a person, contingent through additional external support.

Incidentally it is pointed out that ISO 26262 defines the state of the art. It is not to be conceived as a sufficient minimum standard (Duisberg & Appt, 2010, S. 218).

3.7 European Statement of Principles on Human Machine Interface (ESoP)

The "European Statement of Principles on Human Machine Interface", published 22.12.2006 by the European Union is giving considerations? to the human-machine interface design (HMI) for In-vehicle information and communication systems. It is an updated version replacing the previous from 1999 and is developed by the Commission of the European Communities of 2006. (eSafety HMI WG, 2005)

The European Commission intends the pressure groups at member states to comply with the attached updated recommendation and to enter into a voluntary agreement on this matter.

The guidelines summaries security-relevant aspects although many of the approached issues are also transferable for the design of driver-information systems.

Positive about the ESoP-Guidelines is that the explanations are always connected with positive and negative examples, which makes them very understandable. The relevant standards are given as references as well. To avoid blocking future developments, they are expressed independent of any special technologies.

There are five overall design principles:

- **Design goal 1:**
  „The system supports the driver and does not give rise to potentially hazardous behavior by the driver or other road users."
- **Design goal 2:**
  „The allocation of driver attention while interacting with system displays and controls remains compatible with the attentional demand of the driving situation."
- **Design goal 3:**
  "The system does not distract or visually entertain the driver."
- **Design goal 4:**
  "The system does not present information to the driver which results in potentially hazardous behaviour by the driver or other road users."
- **Design goal 5:**
  "Interfaces and interface with systems intended to be used in combination by the driver while the vehicle is in motion are consistent and compatible."

There are further guidelines including principles about ‚installation', ‚information presentation', ‚interaction with displays and controls', ‚interaction with displays and controls' and , information about the system'.

Principles about **malfunctions** of the system are given in the passage "System behavior principles" at point four:

„**Information** should be presented to the driver about current status and any malfunction within the system that is likely to have an impact on safety.*"*

3.8 Summary and legal implications regarding controllability in the light of research projects

In this chapter we showed, that the state-of-the-art in science and technology exerts wide influence to the assessment of product liability laws in case of an existing product defect to the controllability.

Definitions for the controllability can be found in technical standards like ISO 26262 or codes of practice like RESPONSE 3.

Additionally, in the context of product liability it is important, if the not-intended use of a product in a single case can be seen as a predictable misuse or an user-intended malpractice. In the first case, the manufacturer has to implement constructive and instructive actions regarding the coverage of product liability laws. In the second one, the user is responsible for the misuse.

The implementation of appropriate constructive and instructive actions can enhance the controllability and, at the same time, can be used for coverage of product liability laws.

From a legally perspective important is also the fact, that on the one hand the jurisdiction imposes some specific requirements on the human driver ("optimal driver") and on the other hand, appreciates some privileges under certain circumstances (moment of shock, human error in one moment).

With respect to the requirements of the verification of controllability, the given legal framework of legislation and jurisdiction, which classifies the human driver, should be included in an appropriate way.

4 References

AALA CMU Ambient Assisted Living Association (2013). Guide for Applicants Ambient Assisted Living Joint Programme Call 6. http://www.aal-europe.eu/wp-content/uploads/2013/02/Guide_for_Applicants_20130211final.pdf . Last accessed 2014-11-25

European Commission (2013). Ethics for researchers - Facilitating Research Excellence in FP7. http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf . Last accessed 2014-12-04

European Commission (2012). Why do we need an EU data protection reform? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf . Last accessed 2014-12-05

European Commission (2014). Commission decisions on the adequacy of the protection of personal data in third countries. http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm . Last accessed 2014-12-04

European Parliament; Council of the European Union (1995). Directive 95/45/EC of the European Parliament and of the Council. Official Journal of the European Communities No. L281/31.

European Parliament; Council of the European Union (2002). Directive 2002/58/EC of the European Parliament and of the Council. Official Journal of the European Communities No. L201/37.

Field, Andy (2009). Discovering statistics using spss. Third Edition. London/ Thousand Oaks/ New Delhi/ Singapore: SAGE Publications.

Italian Data Protection Authority (2004). Data Protection Code - Legislative Decree no. 196/2003. http://www.garanteprivacy.it/home_en/italian-legislation . Last accessed: 2014-12-04

juris (2013). Federal Data Protection Act. http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0009 . Last accessed: 2014-12-04

Trans.Safe (2013). Description of Work AAL-6-2013-64.

UNESCO; MOST (2003). Ethical Guidelines – for International Comparative Social Science Research in the framework of MOST. http://www.unesco.org/most/ethical.htm . Last accessed 2014-12-05

WMA – Word medical association (2013). WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects. http://www.wma.net/en/30publications/10policies/b3/ . Last accessed 2014-12-19

Youse GmbH (2013). Toolbox-Methods of User Integration for AAL Innovations. http://www.youse.de/documents/nYOUSE/AALA_ToolboxA4_online.pdf . Last accessed 2014-12-03

Knapp, A. (2006). *ADAS evaluation concepts for system specification.* RESPONSE 3, Final Workshop. Stuttgart, 26. / 27. September 2006.

Becker, S., Brandenburg, K., Feldges, J., Fowkes, M., Johanning, T. & Kopf, M. (2000). *System, user and legal aspects:The integrated approach for the assessment of Driver Assistance Systems.* RESPONSE 1 - Deliverable D2.1.

Becker, S., Brockmann, M., Jung, C., Mihm, J., Schollinski, H.-L., Schwarz, J. & Winkle, T. (2004). *RESPONSE 2 - Final Report: ADAS - from market introduction scenarios towards a code of practice for development and evaluation.* RESPONSE 2 - Deliverable D4.

RESPONSE Consortium. (2006). *Code of practice for the design and evaluation of ADAS.* RESPONSE 3: a PReVENT Project.

Appendix A

Relevant sections of the EU Directive 95/46/EC

Chapter 2 General Rules on the Lawfulness of the Processing of Personal Data

Section I

Article 6

4.1.1.1 Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible wirth those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provice appropriate safeguards;

(c)

Appendix B

Actions and Tasks within the development process according to recommendations of RESPONSE 3 (vgl .RESPONSE Consortium, 2006).:

MAIN PHASE: CONCEPT PHASE			
1 Definition phase: Draft HMI concept and controllability safety concept			
1.1 ADAS functionality	Assign function name		Introduce a suitable name for the ADAS function
	Draft functionality	A	Define system status, modes, transitions and actions
			Characterise situational limits and initial sensor requirements
			Sketch system behaviour under situational limits
			Clarify interactions with other systems
1.2 HMI	Draft HMI interaction	A	Sketch driver activities to operate the system
			Characterise transferred information
			Define take over procedures
	Draft physical layout	A	Consider an integration of the HMI concept in the vehicle
			Draft controls and displays (system input and output)
1.3 Usage	Define domain	A	Characterise the intended market for the ADAS
			Describe the type of vehicle for which the ADAS is intended
			Draft the environment and roads in which the ADAS is used
			Characterise the user group of the ADAS
	Characterise use	A	Draft operating scenarios
			Sketch user expectations, misinterpretation, overestimation
	Characterise misuse	A	Draft non operating scenarios
			Identify reasonable foreseeable misuse
			Find possible measures to avoid misuse
1.4 Standards	Ensure conformity	A	Look for relevant standards and regulations
1.5 Preliminary Hazard Analysis and Risk Assessment	Identify hazards	A; B.1	Identify possible hazardous situations and the relevant sources of hazards within the drafted ADAS function for normal operation, system failure and system limits
	Analyse hazards	A.3	Perform hazard analysis paying specific attention to the controllability aspect
	Assess risk	A.3	analyzed hazards

2 Best concept selection			
2.1 HMI concept specification			
2.1.1 Controllability concept	Specify the controllability concept	A; B	Specify HMI interaction based on the draft concept and controllability results from a risk assessment
2.1.2 HMI	Specify system transitions	A	Identify driver initiated transitions that correspond to operator control actions
			Identify system initiated transitions, caused by changing environmental conditions as well as exceeding the system limits
			Identify system initiated transitions, caused by system failure or failures of other interacting systems
	Specify system dialogs	A	Describe the system feedback to the driver for controllability relevant system states and transitions
			Describe the input/output modalities and dialogs
	Specify physical layout	A	Consider controllability aspects of system states and transitions for specification of the controls and displays
2.2 Selection of HMI concept			
2.2.1 Evaluation criteria	Define criteria	A.3; B.3	Define criteria for the evaluation of the concepts considering controllability requirements based on the risk assessment
2.2.2 Selection of concept	Find a best concept	B; A.3	Evaluate the concepts and select the most suitable one according to the defined requirements. Check if the HMI is suitable for the intended task in normal operation, at system limits and with system failures.

3 Proof of concept			
3.1 Preparation of preliminary sign-off			
3.1.1 Review of HM interaction specification (optional)	Define a validation strategy	Ch. 5.6	Document the procedure in a preliminary review plan for the specified HMI interaction concept
	Perform the review	Ch. 5.6	Review the HMI concept specification according to the plan and identify possible problem areas
3.1.2 Further proceeding (optional)	Consider additional tests	B, D	Check for further tests necessary to assess controllability (controllability relevant topics that can be clearly identified as easily controllable, according to the state of the art in the area of human factors, need not be tested.
			Perform necessary tests (in cases of doubt or in lack of experience tests are recommended.
	Document important topics	Ch. 5.6. 2 Activity C; Open Item List (Ch. 4, Fig.3)	Document the achieved results Document the open controllability topics and the required phase of development necessary to perform a certain test
3.2 Controllability preliminary (optional)	Decide on concept sign-off		Sign-Off the HMI concept or initiate appropriate rework

MAIN PHASE: Series Development

4 Detailed HMI Design

. HMI design	HMI architecture		Develop the functional subdivision
			Consider relevant user tasks and activities
			Define input and output by systematically detailing rele- vant system states and transitions and the related inter- actions between driver and system
	Design the physical layout	A	Decide on the appropriate physical layout of the input and output devices (controls and displays)
	Integrate into overall design	A	Integrate ADAS HMI design into overall design regarding priorisation of system outputs (e.g. warnings and mes- sages) in relation to other functions
			Integrate ADAS HMI design into overall design regarding driver workload
4.2 Update H&R		A.3	Update by including information from detailed design of HMI

5 Verification of HMI

	Verify HMI	C	Verify the design based on its specification concerning HMI requirements for system and human performance
	Document verification	Ch. 5.6. 2 Activi- ty C;	Document and report the verification results Initiate necessary further actions if a non-conformance to requirements is found
		Open Item List (Ch. 4, Fig. 3)	Document and report the verification results Initiate necessary further actions if a non-conformance to requirements is found

6. Validation and Sign-off

6.1 Controllability confirmation and final proof

6.1.1 Planning validation scenarios	Identify driving situa-	B.1	Consider the following situations: normal operation, be- haviour at functional limits, behaviour in case of system failures
			Compile a list of relevant driving situations for system validation and build reasonable clusters
6.1.2 Planning approach for final proof	Select the appropri- ate strategy for each scenario	Ch. 4; B.2; B.3; B.4	Controllability confirmation by an independent expert panel
			Controllability check by a test with naive subjects
			Direct recommendation of Controllability Sign-Off by the ADAS Development Team
6.1.3 Final proof	Controllability confir- mation	D	The experts perform the validation strategy, decide if the design has passed an give a recommendation for sign-off
	Document controlla- bility		Document information that is sufficient to reproduce the recommendation for sign-Off (e.g. approach, equipment, assumptions, decisions, test conditions)
			Compile a set of documents to confirm the controllability for the system sign-off. If the documentation is already available a collection of references is sufficient.
			Documents from the risk assessment procedure, i.e. system and HMI concept description, identified hazards, assessed risks, used checklists assumptions
			Controllability related HMI requirements, i.e. require- ments and references to risks
6.2. Sign-Off	Sign-Off the system	F	The responsible person can sign-off controllability.