Adaptive ADAS to support incapacitated drivers Mitigate Effectively risks through tailor made HMI under automation

Deliverable 10.3 – *Ethics Manual*

Work Package No.	WP10
Work Package Title	Management
Activity No.	A10.3
Activity Title	Quality Assurance Control & Ethical considerations
Dissemination level	PU = Public
Main Author(s)	Jansson, Anders (UU) Anund, Anna (VTI) Pia Brink (VTI) Katerina Touliou (CERTH/HIT)
File Name	ADASANDME_Deliverable_10.3_Final.doc
Online resource	http://www.adasandme.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688900

Version History

Date	Version	Comments
24 November 2016	0.1	First draft ready by Anna Anund and Pia Brink at VTI
23 December	0.2	Input received from Anders Jansson, UU
29 December 2016	0.3	Revisions made by Anna and send to Anders Jansson, UU for comments
24 January 2017	0.4	Revisions and comments included from Ford, Ducati, SE, CERTH
25 January 2017	1.0	Send for peer review
27 February 2017	2.0	Regions made according to comments from CQIR

Authors (full list)

Jansson, Anders, Uppsala Universitet (UU)
Anund, Anna, Statens väg och transportforskningsinstitut (VTI)
Brink, Pia, Statens väg och transportforskningsinstitut (VTI)
Katerina Touliou (Etniko Kentro Erevnas Kai Technologikis Anaptyxis) (CERTH HIT)

Project Coordinator

Dr. Anna Anund
Research Director / Associate Professor
VTI - Olaus Magnus väg 35 / S-581 95 Linköping / Sweden
Tel: +46-13-20 40 00 / Direct: +46-13-204327 / Mobile: +46-709 218287
E-mail: anna.anund@vti.se

Legal Disclaimer

Table of Contents

Index of Figures

Index of Tables

Glossary

ADAS	Advanced Driver Assistance Systems
ADAS&ME	Adaptive ADAS to support incapacitated drivers Mitigate Effectively risks through tailor made HMI under automation
EB	Ethics Board
QM	Quality Manager
IF	Incidental Findings

Executive Summary

ADAS&ME is a user oriented project where the participation of humans is essential for a successful outcome. A sound and correct ethical treatment of participants is therefore of great importance for ADAS&ME. The objective of this deliverable is to specify and structure the ethical procedures to guarantee a sound and correct ethical treatment of human participants. The content of the deliverable is also aligned with the Requirement No. 1 from ECHR.

The deliverable cover ADAS&ME ethics, ethical declarations and conventions of importance, the Partner's responsibilities, the role of the Ethics board, overall ethical principles, ethical principles in ADAS&ME and Data privacy policies. In Chapter 4 partners responsibilities are clearly defined.

1 Introduction

ADAS&ME is a user oriented project where the participation of humans is essential for a successful outcome. A sound and correct ethical treatment of participants is therefore of great importance for ADAS&ME. To achieve this, one part of the management structure involves an ethical board (EB) led by the coordinator and the technical manager. The purpose of the EB is to ensure that the planned evaluations and tests follow international and respective national regulations. In ADAS&ME, tests and evaluations with human participants involved are taking place in five countries (Sweden, Germany, Spain, Italy and Greece).

The objective of this deliverable is to specify and structure the ethical procedures to guarantee a sound and correct ethical treatment of human participants. The content of the deliverable is aligned with the EC H – Requirement No 1.

2 Introduction to ADAS&ME Ethics

2.1 ADAS&ME Ethics Policy

ADAS&ME research will be continuously monitored by the EB of the project, led by the Coordinator and Technical Manager. ADAS&ME will strictly follow the opinions of expert committees in the field (e.g. the European group on ethics (EGE) in science and new technologies to the European Commission and the statement by the Ethics Committee of the American Psychological Association). All national legal and ethical requirements of the relevant directives where the research is performed will be fulfilled.

3 Ethical Declarations and Conventions

3.1 European level

The legislation, regulation and ethical codes named below will be considered; they are defined, and it is described how they are met in terms of processes, timing and responsibilities. ADAS&ME Ethics (and Quality Control) Board will oversee the ethical concerns involved in the project. They will consider the relevant laws and directives on ethical issues and personal data protection in the field, see *Table 1*.

Table 1: Laws and directives to be considered (as a minimum) by ADAS&ME Ethics Board.

Ethical & Social risk	Ethical field	Law/directive
Human dignity and integrity of user	Human Rights	▪ European Convention for the Protection of Human Rights and Fundamental Freedoms ▪ Charter of Fundamental Rights of the European Union, the strongest international / EU / national / institutional regulations shall apply.
Privacy	Data protection	▪ Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe) ▪ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EU) NO 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the EU Cookie Directive) ▪ Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector ▪ Directive 95/46/EC of the European parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ▪ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ▪ Directive 2011/24/EU on the application of patients' rights in cross-border healthcare

Ethical & Social risk	Ethical field	Law/directive
Bioethics and clinical trials	Medical research	▪ Directive 2001/20/EC of the European Parliament and of the council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use (the Clinical Trials Directive) ▪ Regulation EU No 536/2014 of the European Parliament and of the Council of clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (the New Clinical Trial Directive) ▪ Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine ▪ Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use
New technologies	Liability and Safety	▪ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and the market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 ▪ Decision 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (the General Product Safety Directive) ▪ Decision 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC. ▪ Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC

The ethical guidelines and regulations reported in the following sections are applicable for the project progress, and not for the use of the final product of ADAS&ME. Ethics can be defined as "a system of principles governing morality and acceptable conduct" [1] or "the study of fundamental principles that defines values and determines moral duty and obligation[2]". However, in this context, a wider and more specific definition is required. Specifically, the rights that are protected, needs to be identified, as well as the reasons for which these are protected.

The ethical guidelines, provided in the following sections, are written in accordance with the following EU legislation and guidelines:

Human dignity and integrity of user

[1] http://wordnet.princeton.edu/perl/webwn?s=ethics
[2] www.science.psu.edu/alert/frontiers/Glossary1-2001.htm

- **European Convention for the Protection of Human Rights and Fundamental Freedoms**

The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, was opened for signature in Rome on 4 November 1950 and came into force 3 September 1953. It was the first instrument to give effect to certain of the rights stated in the Universal Declaration of Human Rights and make them binding.

The Convention sets several fundamental rights and freedoms (right to lift, prohibition of torture, prohibition of slavery and forced labour, right to liberty and security, right to a fair trial, no punishment without law, right to respect for private and family life, freedom of thought, conscience and religion, freedom of expression, freedom of assembly and association, right to marry, right to an effective remedy, prohibition of discrimination).

Parties undertake to secure these rights and freedoms to everyone within their jurisdiction. The Convention also establishes an international enforcement machinery. To ensure the observance of the engagements undertaken by the Parties, the European Court of Human Rights in Strasbourg has been set up. It deals with individual and inter-State petitions.

- **Charter of Fundamental Rights of the European Union**

The Charter of Fundamental Rights of the European Union, 2012/C 326/02, brings together in a single document the fundamental rights protected in the EU. The Charter contains rights and freedoms under six titles: Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice. Proclaimed in 2000, the Charter has become legally binding on the EU with the entry into force of the Treaty of Lisbon, in December 2009.

The rights of every individual within the EU were established at different times, in different ways and in different forms. For this reason, the EU decided to clarify things and to include them all in a single document which has been updated in the light of changes in society**,** social progress and scientific and technological developments.

The Charter entrenches:

- all the rights found in the case law of the Court of Justice of the EU;
- the rights and freedoms enshrined in the European Convention on Human Rights;
- other rights and principles resulting from the common constitutional traditions of EU countries and other international instruments.

The Charter sets out a series of individual rights and freedoms. The Charter is a very modern codification and includes 'third generation' fundamental rights, such as:

- data protection;
- guarantees on bioethics; and
- transparent administration.

The Charter is consistent with the European Convention on Human Rights adopted in the framework of the Council of Europe: when the Charter contains rights that stem from this Convention, their meaning and scope are the same.

Privacy

- **Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe)**

This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate, at the same time the trans frontier flow of personal data.

In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

- **Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EU) NO 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the EU Cookie Directive)**

The EU Cookie Directive is amended privacy legislation designed to increase consumer protection. The EU Cookie Directive requires websites to obtain informed consent from visitors before they store information on a computer or any web connected device. This is storage is mostly done by cookies, which can then be used for tracking visitors to a site.

The previous privacy legislation required websites to give users information on how they could remove or opt-out of cookies, which was commonly placed in privacy policies that went mostly unread. With the EU Cookie Directive the user of a site will now be required to opt-in when using a website containing cookies. Hence, the website has to block cookies, until visitors have given their informed consent to their use.

The EU Cookie Directive (Directive 2009/136/EC of the European Parliament and of the Council) is an amendment of the Directive 2002/58/EC, which concerns the protection of data and privacy on the web.

- **Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector**

This Directive is concerning the processing of personal data and the protection of privacy in the electronic communications sector. The Directive sets out rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. It also bans unsolicited communications where the user has not given their consent.

The Directive 2002/58/EC will be repealed by a new ePrivacy Regulation. On January 10th, 2017, the European Commission made a proposal for a Regulation on Privacy and Electronic Communications aiming at reinforcing trust and security in the Digital Single Market by updating the legal framework on ePrivacy. The proposed Regulation on Privacy and Electronic Communications will increase the protection of people's private life and open up new opportunities for business. The legal form of a Regulation will ensure that the rules for processing personal data and protecting privacy in the electronic communications sector are identical throughout the EU.

- **Directive 95/46/EC (the Data Protection Directive)**

EU Data Protection Directive is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Directive 95/46/EC encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive is based on the 1980 OECD "Recommendations of the Council Concerning guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data."

These recommendations are founded on seven principles, since enshrined in EU Directive 95/46/EC:

- Notice: data subjects whose data is being collected should be given notice of such collection.
- Purpose: data collected should be used only for stated purpose(s) and for no other purposes.
- Consent: personal data should not be disclosed or shared with third parties without consent from its subject(s).
- Security: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- Disclosure: data subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
- Access: data subjects should be allowed to access their data and make corrections to any inaccuracies.
- Accountability: data subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

In the context of the Directive, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Article 2a). Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link. Examples of such data include address, bank statements, credit card numbers, IP addresses and so forth. Processing is also broadly defined and involves any manual or automatic operation on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction (paraphrased from Article 2b). The Directive is to be repealed and "replaced" by the General Data Protection Regulation (see below).

- **Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive)**

The Data Retention Directive was a Directive issued by the European union and related to telecommunications data retention. According to the directive, member states will have to store citizens' telecommunications data for a minimum of 6 months and at most 24 months. Under the directive the police and security agencies will be able to request access to details

such as IP address and time of use of every email, phone call and text message sent or received. A permission to access the information will be granted only by a court.

- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (The General Data Protection Regulation, GDPR)**

The General Data Protection Regulation is a regulation by which the European Parliament, the Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by harmonizing the regulation within the EU. When the GDPR takes effect it will replace the data protection directive (Directive 95/46/EC) from 1995. Perhaps confusingly for some, there is a new directive as well as a new regulation; it will apply to police procedures, which will continue to vary from one Member State to the other.

The adopted new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 4% of worldwide turnover." The Parliament's version contains increased fines up to 5%. After negotiations between the European Parliament, the European Commission and the Council of Ministers, there is general consensus on the wording of the GDPR and also the financial penalties for non-compliance.

The regulation was adopted on 27 April 2016. It enters into application 25 May 2018 after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by national governments.

- **Directive 2011/24/EU on the application of patients' rights in cross-border healthcare**

The Directive 2011/24/EU sets out the conditions under which a patient may travel to another EU country to receive safe and high quality medical care and the cost must be reimbursed by their own health insurance scheme. The directive also encourages cooperation between national healthcare systems.

Bioethics and medical trials

- **Directive 2001/20/EC of the European Parliament and of the council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use (the Clinical Trials Directive)**

The Clinical Trials Directive is a European Union directive that aimed at facilitating the internal market in medicinal products within the European Union, while at the same time maintaining an appropriate level of protection for public health. It seeks to simplify and

harmonize the administrative provisions governing clinical trials in the European Community, by establishing a clear, transparent procedure. The Clinical Trials Directive is a European Union directive that aimed at facilitating the internal market in medicinal products within the European Union, while at the same time maintaining an appropriate level of protection for public health.

- **Regulation EU No 536/2014 of the European Parliament and of the Council of clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (the new Clinical Trials Directive)**

All clinical trials performed in the European Union are required to be conducted in accordance with the Clinical Trials Directive until the new Clinical Trials Regulation (CTR) EU no. 536/2014 will become applicable, which will be no earlier than 28 May 2016. For further information please see the information on the Clinical trials Directive and the transition period.

The new Clinical Trials legislation, which was adopted on 16 April 2014 and entered into force on 16 June 2014, has taken the legal form of a Regulation. This will ensure that the rules for conducting clinical trials are identical throughout the EU. This is vital to ensure that Member States, in authorizing and supervising the conduct of a clinical trial, base themselves on identical rules.

The Clinical Trials Regulation aims to create an environment that is favorable for conducting clinical trials, with the highest standards of patient safety, for all EU Member States.

Transition period

Until the Clinical Trials Regulation EU No 536/2014 will become applicable, all clinical trials performed in the European Union are required to be conducted in accordance with the Clinical Trials Directive. This Directive will be repealed on the day of entry into application of the Clinical Trial Regulation. It will however still apply three years from that day to:

- ✓ Clinical trials applications submitted before the entry into application (no earlier than 28 May 2016);
- ✓ Clinical trials applications submitted within one year after the entry into application if the sponsor opted for old system.

- **Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine**

The Convention is the first legally-binding international text designed to preserve human dignity, rights and freedoms, through a series of principles and prohibitions against the misuse of biological and medical advances. The Convention's starting point is that the interests of human beings must come before the interests of science or society. It lays down a series of principles and prohibitions concerning bioethics, medical research, consent, rights to private life and information, organ transplantation, public debate etc.

It bans all forms of discrimination based on the grounds of a person's genetic make-up and allows the carrying out of predictive genetic tests only for medical purposes. The treaty allows genetic engineering only for preventive, diagnostic or therapeutic reasons and only where it does not aim to change the genetic make-up of a person's descendants. It prohibits the use of techniques of medically assisted procreation to help choose the sex of a child, except where it would avoid a serious hereditary condition.

The Convention sets out rules related to medical research by including detailed and precise conditions, especially for people who cannot give their consent. It prohibits the creation of human embryos for research purposes and requires an adequate protection of embryos where countries allow *in-vitro* research.

The Convention states the principle according to which a person has to give the necessary consent for treatment expressly, in advance, except in emergencies, and that such consent may be freely withdrawn at any time. The treatment of persons unable to give their consent, such as children and people with mental illnesses, may be carried out only if it could produce real and direct benefit to his or her health.

The Convention stipulates that all patients have a right to be informed about their health, including the results of predictive genetic tests. The Convention recognises also the patient's right not to know. The Convention prohibits the removal of organs and other tissues which cannot be regenerated from people not able to give consent. The only exception is, under certain conditions, for regenerative tissue (especially bone marrow) between siblings.

- **Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use**

The Directive 2001/83/EC brings together all the existing provisions in force on the sale, production, labelling, classification, distribution and advertising of medicinal products for human use in the EU. Some of the key points are that all medicines offered for sale in the EU must have prior authorisation from either a national authority or the European Medicines Agency, and to receive authorisation, manufacturers must provide a range of detailed therapeutic information about the product, including any possible side-effects.

New technologies

- **Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and the market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93**

This Regulation lays down clear rules on the organisation and operation of accreditation, within the European Union (EU), of conformity assessment bodies responsible for performing evaluation tasks to ensure conformity with the applicable requirements. It is important to guarantee a high level of market surveillance in order to satisfy the requirements of protection of public interest such as health and safety in general, health and safety in workplace, protection of consumers, the environment and security. Accreditation is the final public control step within the conformity evaluation system and attests to the technical competence of the conformity evaluation bodies. It also contains rules on CE marking.

These rules reinforce the existing system, without weakening existing instruments such as the General Product Safety Directive, which has on the whole been successful.

- **Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (the General Product Safety Directive)**

The General Product Safety Directive requires firms to ensure that items on sale are safe and to take corrective action when that is found not to be the case. It introduces an EU rapid alert system for dangerous non-food products. This enables national authorities to share

information promptly on any measurements taken to withdraw such products from sale. Some of the key points are that products placed on the EU market must be safe, and the products must bear information enabling them to be traced, such as the manufacturer's identity and a product reference.

- **Decision 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC**

The decision sets out common principles and procedures which EU legislation must follow when harmonising conditions for marketing products in the EU and the European Economic Area. It also includes reference requirements to be incorporated whenever product legislation is revised. As such, it is a template for future product harmonisation legislation. Some of the key points are that the decision provides clear definitions for relevant terms, such as 'manufacturer', 'placing on the market', 'recall' or 'withdrawal' of products, it also shows clear divisions of responsibility are set for manufacturers, importers and distributors along the product chain.

- **Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC**

The objective of this Regulation is to improve the free movement of goods in the Community. It establishes rules and procedures which should be followed by the authorities of Member States when they take or intend to take a decision which could hinder the free movement of a product lawfully marketed in another Member State and not covered by harmonised rules at Community level. It applies from 13 May 2009.

3.2 International level

In addition to the aforementioned EU regulations, the following international conventions and declarations have been taken into consideration:

- **Universal Declaration of Human Rights**

The Universal Declaration of Human Rights is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948. The declaration consists of 30 articles that states that all men are born free and equal, we all have the right to life, and to live in freedom and safety. We are all equal before the law, and our human rights are protected by law.

- **World Medical Association Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects**

The World Medical Association (WMA), an international organization of physicians, was formally established on September 17, 1947, pursuant to the resolutions of the First General Assembly of WMA held in Paris, France. In 2007, the WMA had a membership of 84 national medical associations and represents some 9 million physicians. The goal of the

World Medical Association is to serve humanity by endeavouring to achieve the highest international standards in medical education, science, ethics, and health care for all peoples of the world.

- **Universal Declaration on Bioethics and Human Rights (UNESCO)**

Since the 1970s, the field of bioethics has grown considerably. While it is true that bioethics today includes medical ethics issues, its originality lies in the fact that it goes much further than the various professional codes of ethics concerned. It entails reflection on societal changes and even on global balances brought about by scientific and technological developments. To the already difficult question posed by life sciences – How far can we go? – other queries must be added concerning the relationship between ethics, science and freedom.

- **The Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine, signed in Oviedo on 4 April 1997, (the Oviedo Convention)**

This Convention is the only international legally binding instrument on the protection of human rights in the biomedical field. It draws on the principles established by the European Convention on Human Rights, in the field of biology and medicine. It is a framework Convention aiming at protecting dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine.

- **UN Convention on the Rights of the Child, 2002**

The United Nations Convention of the Rights of the Child is a legally-binding international agreement setting out the civil, political, economic, social and cultural rights of every child, regardless of their race, religion or abilities. Since it was adopted by the United Nations in November 1989, 194 countries have signed up to the UNCRC, with only two countries in the world still to ratify. All countries that sign up to the UNCRC are bound by international law to ensure it is implemented. This is monitored by the Committee on the Rights of the Child.

Under the terms of the convention, governments are required to meet children's basic needs and help them reach their full potential. Central to this is the acknowledgment that every child has basic fundamental rights. These include the right to life, survival and development; protection from violence, abuse or neglect; an education that enables children to fulfil their potential; be raised by, or have a relationship with, their parents and to express their opinions and be listened to.

- **Universal Declaration on the human genome and human rights adopted by UNESCO**

The Declaration is a document that was issued by UNESCO in 1997 and is perhaps best known for its statement against human cloning and abuse of human genome against human dignity.

4 Partners responsibilities

The following project partner regulations related to compliance, approvals, privacy, personal health information and collaboration within the project shall apply:

1. Each party shall be responsible for ensuring its own compliance with all laws and regulations applicable to its activities. Such laws include, but are not limited to, those in respect of rights of privacy, intellectual property rights and healthcare.
2. Each party represents that it has all necessary third party, hospital and/or patient explicit consents to permit distribution and use of the data (including medical data) and any other information provided to other parties.
3. Any party which provides any data or information to another party in connection with the project will not include any personal information relating to an identified or identifiable natural person or data subject.
4. To this end, the providing party will anonymise all data delivered to other parties to an extent sufficient to ensure that a person without prior knowledge of the original data and its collection cannot, from the anonymised data and any other available information, deduce the personal identity of subjects.
5. Each party shall be solely responsible for the selection of specific database vendors/data collectors/data providers, and for the performance (including any breach) of its contracts between it and such database vendors/data collectors, (to which no other project partner shall be a party, and under which no other partner assumes any obligation or liability) and shall further warrant that it has the authority to disclose the information, if any, which it provides to the other parties, and that where legally required and relevant, it has obtained appropriate informed consents from all the individuals involved.
6. Partners supplying special data analysis tooling, shall have the right on written notice and without liability to terminate the license that it has granted for such tooling to be used in connection with the project, if the supplying partner knows or has reasonable cause to believe that the processing of particular data through such tooling infringes the rights (including without limitation privacy, publicity, reputation and intellectual property rights) of any third party, including of any individual.

5 The role of the Ethics Board

5.1 ADAS&ME Ethics Board

The Ethics Board will be responsible the project's Ethics Board (composed of three external members, the Coordinator, Technical and Ethics Managers) and will act as supervisors of the ethical activities of the project and the local ethics committees at each pilot site. They will do so in order to take into account both European and national ethical and legal requirements.
The ADAS&ME Ethics Board has a duty to:

- Protect private and sensitive information and ensure that participants will not be harmed during the pilots. Collected data will be anonymous and treated as confidential i.e information that will be handled with extra care and not at any point connected to sensitive information about the participant.
- Respect participant's free will and treat them as intelligent beings who decide for themselves about any type of gathered data that are indeed outcomes of their participation.
- Inform in full about which data will be collected and how data will be collected, processed, shared, and disposed before signing the consent form.
- Communicate their findings through open-access journals to other researchers and academic communities (especially true if it is requested by the funder).

All used assessment tools and protocols within ADAS&ME pilots will be verified beforehand by its Ethics Board, regarding their impact to users' well-being before being applied to the pilot sites. At least three renowned experts in the field, chaired by an experienced ethics coach, constitute the project Ethical Board, assisted by further external experts, if needed. The Ethics Board works for implementing and managing the ethical and legal issues of all procedures in the project, ensuring that each of the partners provides the necessary participation in ADAS&ME and its code of conduct towards the pilot participants. The Ethics Board constantly updates the Ethics and Privacy Protection Manual (ethics code of conduct of research), leading to the recognition of key ethical and legal issues. Especially the core ethical issues will be tackled. The members of the Ethics Board are the following:
The ethics board consists of three key experts with a long record of tests/evaluations involving humans and are trained in ethical concerns.

Dr. Torbjörn Åkerstedt, Karolinska Institutet, Sweden
Professor in Psychology, Karolinska Institutet, and Director of the Stockholm Stress Center. Former President of the European Sleep Research Society and General Secretary of the World Federation of Sleep Research and Sleep Medicine Societies.

Dr. Anders Jansson, Uppsala Universitet, Sweden
Professor in Human-Computer Interaction, Associate Professor in Psychology, Uppsala University. Researcher specializing in Human Factors, Cognitive Ergonomics and Human-Automation Interaction, and the leader of the Technology in Human Reasoning (TiHR) Group.

Dr. Michal Regan, ARRB, Australia
Professor, Australian Road Research Board (ARRB Group), Chief Scientist in Human Factors & Safe Systems Department, Adjunct Professor University of NSW in Sydney, Australia.

5.2 Ethical Management and Control of pilot sites

The diagram in Figure 1 presents the procedure of ethical considerations from planning to realisation of a test/evaluation. The EB will supervise and ensure that the ethics guidelines of the project are followed, this is done in close collaboration with the Evaluation Manager (WP7 leader). The responsible partner and the principal investigator / researcher for a test / evaluation will be responsible for the submission and approval of the pilot research protocol to the local/regional and/or institute ethics' Board required in each country. The external members of the EB are all persons with valuable experience in projects related to pilot testing and evaluations with humans. The QM of ADAS&ME is the one responsible for keeping track of the process.

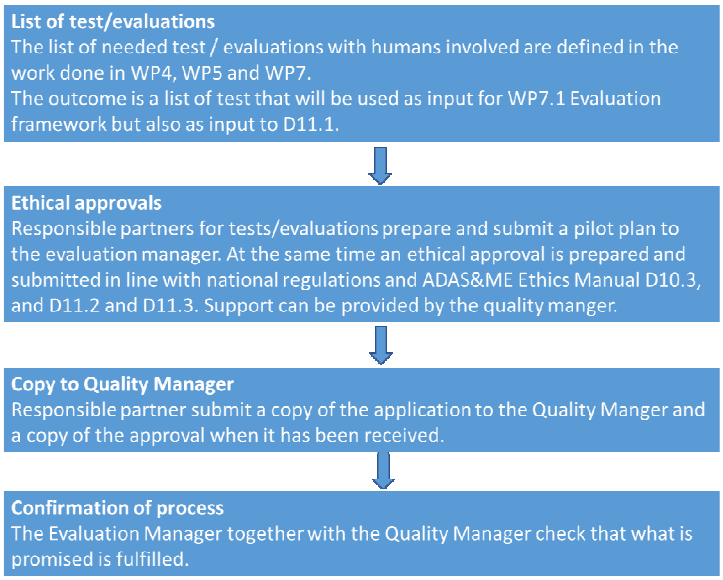

Figure 1: The procedure and flow of information from ethics board to pilot site.

6 Overall Ethics policy

6.1 Ethics in relation to participants

As a researcher, it is your personal responsibility to carry out your research in an ethical manner. Research is not primarily for the embellishment of the researcher, the profit of a company or the political aims of the government. Each individual scientist, in each research project and each project phase, must make thoughtful judgements of how best to contribute to science, humanity and human welfare. In order to do that, ethical principles developed to help guide researchers in their everyday research tasks.

Research is a process of inquiry. In the procedures or design phase of a research project, the researcher must examine the research plans potential ethical issues and take steps to correct them and must do so prior to contacting any participants. The proposed research plan, and how it puts into practice, must survive ethical evaluation in advance; if an ethical problem exists, the researcher must modify the plan. Only when the plan can stand up to ethical challenges can the investigator in order to start or proceed to the next phase.

Ethical researchers must address the issues of explicit and informed consent, confidentiality, safety, deception, debriefing, security and diversity in their research with human participants. It is your task as a researcher to think these issues through in order to find out whether your participants will experience and perhaps react negatively on any of these issues. Below (chapter 6.2) is a checklist before you begin your study.

6.2 Ethical checks before beginning a study

1. Is the proposed research adequately designed, so that it will be of informational value?
2. Does the research pose risks of physical or psychological harm to participants by using deception, obtaining sensitive information or exposing them for risks in terms of safety and/or security hazards?
3. If risks exist, does the research adequately control these risks by including procedures, such as debriefing, removing or reducing risks of physical harm, or obtaining data anonymously? If that is not possible, will the research procedures guarantee that information will remain confidential?
4. Is there a provision for obtaining explicit and informed consent from all participants? Will the researcher provide sufficient information to potential participants so that they will be able to give their explicit and informed consent? Is there a clear agreement in writing (the informed consent form) between the researcher and the potential participants? The explicit and informed consent should also make it clear that the participant has the right to access processed data, to restrict processing, to object from further data processing, to ask for data erasure and is free to withdraw from the study at any time.
5. Will participants receive adequate feedback at the completion of the study, including a debriefing if that is necessary?
6. Do I as researcher accept my full responsibility for the ethical and safe treatment of all participants?
7. Have I as part of the project informed the Ethics Board about the ethical issues I have identified and of which I am aware?

6.3 Ethics in relation to data gathering

Research ethics also apply to the misuse of data. It is your responsibility as a researcher to react and call to attention any form of manufacturing or deliberate falsification of data that has

as its purpose to convey a more positive result compared to what actual data show. Fortunately, such deliberate distortions are rare and often connected to an individual researcher however, one ominous form of data distortion is when industry or governments suppress scientific data in order to convey a certain message that does not have full support in the data gathered and collected.

6.4 Ethics in relation to statistics

Ethical researchers should always use statistics to represent their results accurately and fairly. It is a particularly important ethical obligation to present the findings and the statistics that summarize those findings in a manner that accurately reflects the data. Selecting data that deliberately emphasize some aspects while de-emphasizing other aspects in order to distort the results and mislead people is dishonest and unethical. Such "cherry-picking" the data is unethical scientific behaviour. It can be of particular interest to watch out for such misuse of data when data contain large individual differences.

6.5 Ethics in relation to test situations

The major ethical issues in naturalistic observations and field studies involve explicit and informed consent, confidentiality and researchers' access to sensitive material. The most essential safeguard is explicit and informed consent. This also goes for test/evaluations and control groups. A basic principle in most, if not all, science is that the research and the investigation must do no harm to the participants. This is often easy to understand and possible to imagine. But the second most basic principle is that the research and the investigation must also do some good, and this is not only in some general sense, as a contribution to science and humanity, but also in the very specific case of a particular individual. This is often a neglected aspect, but to be an ethical researcher the researcher must also take this into consideration.

7 Ethical principles for ADAS&ME

7.1 Participants

As defined in Part B section 5 the main target user groups of ADAS&ME are experienced, active, and healthy individuals. The participants have to have the competence to understand the explicit and informed consent information. In the unlikely case that they are unable to do so, they will be excluded from any tests within ADAS&ME.
The scenarios will only include participants with competence to understand the explicit and informed consent information and a valid driving license.
ADAS&ME will not touch any of the following fields of research:

- research activity aiming at human cloning for reproductive purposes,
- research activity intended to modify the genetic heritage of human beings which could make such changes heritable,
- research activities intended to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer.

Furthermore, ADAS&ME does not include any research involving

- the use of human embryonic tissue, human foetuses, human foetal tissue, other human tissues,
- genetic information,
- people unable to give consent,
- pregnant women,
- animals

Research has to be inclusive and representative of different driver types. The selection and recruitment of participants is a crucial part of the involvement process, as it will impact on the quality of the outcomes and the sustainability of the research or policymaking process. At this stage a satisfactory number of users and combination of drivers' characteristics is sought; gender balance and equality is addressed.
ADAS&ME will target drivers in the large sense: Specific inclusion criteria will apply (i.e. at least five years since obtaining driving license, driving more than 10 000 km per year, and using their car at least two times per week; coming from different digital literacy backgrounds with a well-balanced gender sample). Participants will be screened prior recruitment. Participants with mood, personality, sleep disorders and physical impairments are excluded from testing, as also are drivers who are under medication that might affect driving performance (e.g. antidepressants) or the influence of alcohol. The substantial number of users will ensure a wide trial perspective, including: i) different age groups, ii) balanced female/male ratio iii) various social backgrounds. The Ethics Board of ADAS&ME will oversee the selection of participants.

Personal data of participants will be strictly held confidential at any time of the research. This means in detail that:

- Participants will have the ability to give explicit and informed consent to participate;
- No identification data, in terms of name of the person or sensitive data will be available when analysing data;
- All participants will be strictly volunteers;
- Personal data will be anonymised and strictly used for the project purposes;
- No personal data will be centrally stored, without anonymization.

- Participants will receive a copy of their consent form;
- Participants will be briefed (information sheet) and debriefed after their participation;
- Participants will receive monetary compensation appropriate for their time spent during testing;
- Participants will be covered by the institute's / companies insurance when driving the research vehicle and a driver instructor will be always present. All test volunteers will receive detailed oral information. In addition, they will receive in their own language:
- a commonly understandable written description of the project;
- a simple description of the project will be available in both written and oral form;
- the project goals;
- the planned project progress;
- the related testing and examination procedures;
- advice on unrestricted disclaimer rights on their agreement;
- information about face and voice data recordings and the exact reference to the consent form.

A contact person for each of the tests/evaluations will be appointed and will oversee contacts with participants and ethical issues. This person will be responsible to report back to the principal researcher about participant involvement, ethical and data protection issues. On the other hand, the EB will scrutinise the research, to guarantee that no undue risk for the participant, whether technically, or related to the breach of privacy, is possible.
The research team will implement the research project in full respect of the legal and ethical national requirements and code of practice. Whenever authorisations must be obtained from national bodies, those authorisations shall be considered as documents relevant to ADAS&ME. Copies of all relevant authorisations shall be available prior to commencement of the relevant part of the research project.

7.2 Gender issues

In addition to the ethics issues monitoring, the monitoring of the gender level of participation within the project activities is important for ADAS&ME. Equal opportunities and equal treatment between men and women will been guaranteed throughout the following actions:

- creation of equal conditions for men and women with respect to access to employment;
- the reversal of the burden of proof in cases of discrimination;
- positive discrimination to promote the under-represented gender.

In more detail, there is a number of specific European and UN Policies that will be adopted to promote the equity of gender (i.e. Council Directive 75/117/EEC, etc.).

ADAS&ME will ensure that during all its phases, and as much as possible equal gender participation will be maintained; this addresses research and development phases, as well as evaluation phases. The gender will be one of the Pilots and other test/evaluations participants' characteristics that will be tracked and statistically processed (to come up with any correlations if applicable).

7.3 Privacy protection and confidentiality

Only the principal investigator, at each pilot site, will have access to personal information. People who will analyse data will receive anonymised and coded information. Any recorded data will be available only in anonymised format. Participants who will consent for video recording (e.g. face recognition) will participate in testing and their results will be used only for scientific purposes, in an anonymised manner.

Involvement of human participants is ethical, and information will be provided at each stage of involvement for all phases they will be part of. The annexed documents will be further adapted based on the specifics of the final testing protocols. Involvement of end-users is central in ADAS&ME, which will test the ADAS&ME integrated detection/prediction system with adequate number of users across the use cases at each relevant site. These activities and the overall ethical conduct of the project will be supervised by the ADAS&ME Ethics Board including also experts on ethical issues.

The principles of the European Convention of Human Rights, the rules of the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and especially the European Directive 95/46/EC and the Regulation (EU) 2016/679 (decided, but implemented by May 2018), for the protection of personal data will be strictly followed when addressing the ethical questions of ADAS&ME.
Core ethical issues within ADAS&ME are related to:

- Privacy protection and confidentiality
- Explicit and informed consent
- Incidental findings
- Transparency of the collected data management by the final system and during baseline and pilots
- Traffic safety and secure use of sensors
- Risk assessment (Insurance)
- Delegation of control
- Incentives (Financial inducements, etc.)

The proper management of these issues will be carefully investigated and any relevant principles and the main procedures regarding privacy, data protection, security, legal issues and ethical challenges will be defined during both development, testing, and optimisation phases It will be drafted in consultation with the ADAS&ME Ethics Board acting as supervisors of the ethical activities of the project taking into account both European and national ethical and legal requirements.

7.4 Explicit and informed consent

In general
In general terms, explicit and informed consent is the process by which a participant will be fully informed about the research in which he/she is going to participate. It originates from the legal and ethical right that the participant has to direct what happens to his / her body and personal data and from the ethical duty of the investigator to involve the participant in the research. Seeking the consent of an individual to participate in research, reflects the right of an individual to self-determination and also his/her fundamental right to be free from (bodily) interference, whether physical or psychological, and to protect his / her personal data. These are ethical principles recognised by Law as legal rights. A distinction between three explicit and informed consent elements is possible:

- the information given,
- the capacity to understand it and
- the voluntariness of any decision taken.

With respect to the participants, they have the opportunity to choose what will or will not happen to them. This opportunity is provided, when adequate standards for informed consent are satisfied. The written information as well as the sought informed consent corresponds to information gathered from the revised version of the Helsinki Declaration of 1964 (http://www.wma.net/en/60about/70history/01declarationHelsinki/index.html) as lastly amended in Tokyo, 2004, and the Convention of the Council of Europe on Human Rights and Biomedicine (1997). (http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=04/02/2013&CL=ENG).

In seeking explicit and informed consent from a participant, according to international Ethical Guidelines for Biomedical Research, provided by Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the World Health Organization (WHO), involving human subject the following information has to be provided to each participant (http://www.cioms.ch/publications/layout_guide2002.pdf). For ADAS&ME the following are relevant to include.

- The purpose of the research, expected duration, and procedures.
- Their right to decline to participate and to withdraw from the research once participation has begun.
- The foreseeable consequences of declining or withdrawing.
- Reasonably foreseeable factors that may be expected to influence their willingness to participate such as potential risks, discomfort, or adverse effects.
- Any prospective research benefits.
- Limits of confidentiality.
- Incentives for participation.
- Contact details, for questions about the research and research participants' rights.

Guidelines for the investigators gathering explicit and informed consent

The following comments may help investigators on how to provide information to prospective participants and therefore obtain consent:

- Explicit and informed consent is a process, not just a form. Information should be presented to enable persons to voluntarily decide whether or not to participate in ADAS&ME research.
- It is a fundamental mechanism to ensure respect for persons through provision of thoughtful consent for a voluntary act. The procedures used in obtaining informed consent are designed to educate the participant population in terms that they can understand. Therefore, informed consent language and its documentation (especially explanation of the study's purpose, duration, test/evaluations procedures, alternatives, risks, and benefits) must be written in "layman's language" (i.e. understandable by the people being asked to participate). The written presentation of information is used to document the basis for consent and for the participants' future reference. The consent

document will be revised when deficiencies are noted or when additional information will improve the consent process.

- The investigator should be aware of the fact that the use of the first person (e.g., "I understand that ...") can be interpreted as suggestive, may be relied upon as a substitute for sufficient factual information, and can constitute coercive influence over a participant.
- Use of scientific jargon and legalese is not appropriate. The document is primarily thought of as a teaching tool, not as a legal instrument.
- The overall experience that will be encountered must be described.
- The human participants will be informed of the reasonably foreseeable harms, discomforts, inconveniences and risks that are associated with the research activity. If additional risks are identified during the course of the research, the consent process and documentation will be revised to inform participants as they are re-contacted or newly contacted.
- The benefits that participants may reasonably expect to encounter will be described. There may be none other than a sense of helping the public at large.
- The participants are told the extent to which their personally identifiable private information will be held in confidence. See also the chapters about data management, security and privacy.
- If research-related injury (i.e. physical, psychological, social, financial, or otherwise) is possible, that is more than minimal risk, an explanation will be given of whatever voluntary compensation and treatment will be provided (not expected to be the case within ADAS&ME).
- The legal rights of participants will not be waived in any way. The participants should not be given the impression that they have agreed to and are without recourse to seek satisfaction beyond the institution's voluntarily chosen limits.
- Details of contact persons who are able to answer questions of participants about research, rights as a research participant, and research-related injuries will be provided.

A single person is not likely to be appropriate to answer questions in all areas. This is because of potential conflicts of interest or the appearance of such. Questions about the research are most often best answered by the investigator(s). These questions can also be addressed to the investigator, an ethics committee, or other informed administrative body. The informed consent document will contain contact information with local telephone numbers to answer questions in specified areas. A partner that identify a doubt of any of the questions above need to turn to the Quality Manger to inform or for help.

The participation is voluntary and the participant has the right to withdraw at any time, without being obliged to explain the reason of withdrawing. It is important to point out that no penalty or loss of benefits will occur as a result of either not participating or withdrawing at any time of the test/evaluations.

7.5 Incidental findings

Treatment of incidental findings related to driver's health state and or any traffic violations will be included in the informed consent.

Any findings that are related to driver's health (i.e. excessive stress, leading to chronic stress, diagnosis of sleep apnoea, narcolepsy, or other sleep related disorders, etc.) during the tests will be communicated in writing to the test participant and only, supporting them to contact medical support if needed. Such incidental medical findings, as well as any traffic rules' violations during the tests will not be communicated to 3rd parties (including insurances, authorities, etc.); as the driver is driving " as he/she will do when along" and assumes fully legal responsibility on his/her acts. Written exception (included in the informed consent form) will be made for deliberate criminal acts on behalf of the driver or/and related to an eventual accident during the tests.

7.6 Transparency of data collection techniques and management

The informed consent aims at ensuring that the user accepts participation and is informed about all relevant aspects of the research project; it should be given in written form after the users have been provided with clear and understandable information on their role (including rights and duties), the objectives of the research, the methodology used, the duration of the research, the possibility to withdraw at any time, confidentiality and safety issues, risks and benefits.
The basic elements of the ADAS&ME informed consent will include:

1. The objective of the study, its duration and methodology
2. Possible risks, discomforts and side-effects (also related to traffic safety)
3. Privacy and data protection procedures
4. The possibility to decline the offer and to withdraw at any point of the process (and without consequences)
5. Contact person

7.7 Incentive schemes

The participants will receive an incentive as compensation for their participation. It will not be conditional based on performance or restricted to finalization of the actual test. The incentive will be in line with the performing partners general practice.

7.8 Risk assessment and mitigation strategy

Data collection and evaluations should not entail any undue risk for participants.
Testing of technologies is supervised; sensors and systems will be verified and validated prior to any use. The integrated systems do not pose any safety risk for participants, the baseline is the already existing case without a system..

8 Data privacy policy

8.1 Confidentiality and data protection

Only anonymised data will be processed and, therefore, no personal data will be used in relation to specific user. The name of the person will not be connected to other characteristics (e.g. age, sex, nationality and health condition). The connection will be done through a number were the "key" to the participant is . Participants will be recorded only if they provide consent. All this information falls under the European legislation for the lawful processing of personal data.
Special attention is also given to national legislation. These provisions have to be respected even if the users have given their consent for the processing of their personal data. Especially regarding sensitive data, like physical or mental health, sexual orientation and ethnic origin, more restrictions apply.
To avoid risks related to the processing of personal data such as identity theft, discriminatory profiling or continuous surveillance, the principle of proportionality has to be respected. Data can be used only for the initial purpose for which they were collected.
Anonymisation or pseudonymisation is a way to prevent violations of privacy and data protection rules. Processing has to be limited to what is truly necessary and less intrusive means for realising the same end have to be considered. 1.

In ADAS&ME we have identified which data protection rules to apply and establishes a list of risks and potential solutions; taking due account of the following:

- What kind of data will be processed?
- What is the purpose of the processing?
- Will the data exceed the purpose of the study?
- Are there procedures ensuring that data is processed only for the originally identified purposes?
- Who is the owner of the data?
- Is data connected to other information?
- Will data be commercially exploited?What is the duration of the storage of the data?
- Where will the data be stored and according to which national legislation?
- Who will access the data? Are they secured?
- Will the user be recorded?
- Which biometrics will be implemented?
- Who will supervise the data protection?

When 2016/679 is implemented the following needs to be considered.
Before processing any data, ADAS&ME provide the Participants with the following information:

- The identity and the contact details of the data controller and, where applicable, of the controller's representative;
- The nature of the data being processed;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- Their right to lodge a complaint with a supervisory authority.

8.2 Coding anonymized data and storing

In order to obtain valid test results that can be post-processed and analysed, some personal data of the test participants will be collected, anonymized and stored electronically in ADAS&ME. In addition to this personal data, there will be test applications using unobtrusive physiological and/or behavioural measurements in order to get an objective handle on the respective test performance and physiological state of the test persons during task performance.

Personal data on participants will be used in strictly confidential terms and will be published only as integrated statistics (anonymously) and under no circumstances as individual data set. All test data will be anonymized. Only one person per site will have access to the relation between test participants' code and identity, in order to administer the tests. One month after the tests end, this reference will be deleted, thus safeguarding full anonymity. No other identifier will be kept. Nevertheless, stored data will by no means relate to a person's beliefs or political or sexual preferences.

8.3 Security of ADAS&ME system

ADAS&ME information system will be designed to provide the required level of security efficiently. However, it may occur that there will be some conflicts between the several objectives. For example, security interests can conflict with performance objectives. This should not be surprising, since measures to enforce security often increase the size or complexity of a computing system. Security interests may also reduce the ability of the system to provide data to users, by limiting certain queries. Introducing security into ADAS&ME system is therefore a balancing process between providing the desirable level of protection on the one hand and maintaining an adequate level of availability and performance, so that legitimate users have easy access to the data, on the other.

Networking and communication security issues are arisen, since a multitude of different sensors interact with local or remote applications. For ADAS&ME two different networks are defined: the Local Area Network (LAN) and the Wide Area Network (WAN). Data security and privacy concerns are applicable at both levels. It is widely accepted, that security is a basic requirement for the appropriate introduction and use of information and communication technologies. The increasing employment of advanced technologies makes information systems more efficient, yet more complex, posing new challenges to ensure the protection and confidentiality of data and their integrity and availability. The new technologies contribute to improving the efficiency and quality of services to the patient and they are valuable tools for their management.

Current thinking in information systems security is that the issues centre on confidentiality (information is only disclosed to those users who are authorised to have access to it), integrity (information is modified only by those users who have the right to do so), and availability (information and other IT resources can be accessed by authorised users when needed). The risks violating these three security principles cannot be reduced to zero. But a specific balance of risks and effectiveness has to be found in all application systems. The level of security that

should be included in an information system involves therefore some judgement about the dangers associated with the system and the resource implications of various means of avoiding or minimizing those dangers.

There are five steps that should be followed to assure the maximum possible security for ADAS&ME :

- Develop Information Security Policies and Standards.
- Design the Information Security Architecture and Processes.
- Implement Information Security Awareness and Training.
- Implement Information Security Technologies and Products.
- Auditing, Monitoring and Investigating.

On the basis of the above steps, the following general principles related to information systems security has to be taken into consideration by ADAS&ME.

- The security considerations must take into account all system S/W and H/W that touches information flowing into, and out of, the system.
- The security considerations must be achieved by pursuing data protection by design and by default.
- The aim should be at providing adequate level of secrecy (prevent disclosure) and yet preserving integrity and integrity controls (e.g. referential integrity).
- Data integrity is a key requirement. The system must preserve the integrity of the data stored in it. The user must be able to trust the system to give back the same data that is put in the system and to permit data to be modified only by authorised users. The data should not be destroyed or altered either accidentally, as in a system crash, or maliciously, as in some unauthorised person modifying the data. At the very least, the user should know if the data was corrupted.
- Physical integrity, so that the data of the ADAS&ME system is immune to physical problems, such as power failures, and so that it is possible to reconstruct e.g. a database if it is destroyed through a catastrophe.
- Logical integrity, so that the structure of the ADAS&ME databases is preserved. With logical integrity, a modification to the value of one field does not affect other fields, for example.
- Element integrity, so that the data contained in each element is accurate.
- Data should be available when needed. This implies system fault tolerance and redundancy in data, software and hardware. Inference and aggregation must be studied and controlled.
- Audit should be detailed enough to be useful and sufficient enough so as not to severely burden system performance.
- The prototypes should be of general purpose, commercial quality and, according to most proposers, relational systems. The relational system has been chosen because it is currently the model of preference in the commercial world.
- Access control, so that a user is allowed to access only authorised data and so that different users can be restricted to different modes of access (e.g. read or write).
- User authentication, in order to be sure that every user of the ADAS&ME system is positively identified both for the audit trail and for permission to access certain data.

- Availability, so that users can access the ADAS&ME system in general and all the data for which they are authorised.
- Auditability, so that it will be possible to track who has accessed (or modified) the elements in the ADAS&ME databases.

In order to prevent random access and to assure data protection in accordance to national law, it is assumed that the host providing the database and any participating hosts that access it are directly in a secure area. The database area should also be detached from the LAN through a firewall that restricts access to this secured part.

A transaction gateway will be the direct contact for all client requests. It is responsible for a limited access to certain types of information per user (client), for a client authentication and for the prevention of intrusion/tapping (by using well tried encryption methods).

Only by relying on the technical solutions for data protection is not sufficient to ensure its security. The key is to implement a culture of security and confidentiality. It has to be an interdisciplinary approach between all users. The development of policies must be strong enough to protect the system, yet flexible enough not to disrupt the user and negatively affect productivity. When developing the policy document, it is important to build it so that everyone in the system can read and understand it. Policies must include requirements for certain types of documents to be encrypted, the use of digital certificates to ensure authenticity of communications and mandating the use of physical security products while creating the biometric authentication core.

Once policies are in place, the system needs to define the overall processes by which the policies will be implemented, monitored and enforced. Policies become valueless if they cannot be enforced, and enforcement is not feasible without monitoring. There are a number of policy management applications available on the market. The system needs to tread a careful path on this issue, as it is important for the involved partners to understand the value of security.

Once the architecture is in place, the next step is to raise awareness and train the users of the ADAS&ME system. This is the next most important step after policy definition. The majority of security programs fail because users do not use the security products effectively, if at all. Only an awareness program and training can address this issue. The users need to understand why security is critical to the system, and what they do on a day-to-day basis can have serious consequences. The users need to be thoroughly trained on the new security applications, and their use of those applications needs to be monitored to ensure that policies are being adhered to. Only when security is adopted as part of how people utilize the ADAS&ME system and services, will the threat to the system be reduced.

Once the policies are in place, security architecture needs to be structured on the basis of the following elements:

Security Protocols: The security protocols that should be in place in order to secure the communication channels. The use of Secure Authentication Protocol (SAP) between any communicating entities is proposed for ADAS&ME.

In the framework of ADAS&ME, for example, WLAN security is a major issue. At the most basic level, wireless security requires Authentication (that only authorized users have access

the network) and Encryption (information passed on the network can be read only by the intended recipient and without tampering). Various possibilities exist in the new standards for WLAN security regarding the authentication process. (SAP) is a simple and secure authentication protocol which can be used in small to medium networks and can provide a simple authentication. It is simple to implement and provides authorization in addition to secure authentication.

Moreover, the Secure Sockets Layer (SSLv3) protocol is also proposed, which is known to be as safe as the underlying encryption algorithms (SSL itself does not imply the use of specific algorithms, but rather provides a secure frame for initial authentication and key exchange).

SSL is also widely spread and readily available on most operating systems. SSL requires two different algorithms, one symmetrical algorithm for the actual data encryption and another (asymmetrical algorithm) to exchange the single symmetrical encryption key used on both sides of the communication. Only a very limited number of asymmetrical encryption algorithms exists – nearly all of them sharing more or less the same strategies. RSA is the only commonly used algorithm – we recommend a key length of 1024 bits or higher, which is at present known to be impossible to hack in a reasonable amount of time (several millions of years using brute force on currently available equipment). A wider range of symmetrical algorithms is available, which differ in two relevant aspects: speed and strength. RC4 is considered a good balance, being simple, very fast and providing a similar strength to RSA/1024 using a key length of 128 bits.

Other algorithms may be taken into consideration, like IDEA or DES, both requiring somewhat more CPU time. SSL allows for negotiation of feasible algorithms at connection time.

SSL also requires at least a server-side authentication, allowing the client to be sure, it is communicating with the expected host. An SSL-server may also request the client to authenticate itself through a signed X.509 certificate. This two-way authentication guarantees a perfectly safe communication between server and client, but may not – under all circumstances – be possible.

An alternative method is username/password authentication. After establishing a secure SSL communication between server and client, the client can send a username/password combination to the server. Since encryption is active, it is not possible for an intruder to read the contents of an authentication packet, though it is possible to implement a challenge authentication method as an additional measure, to allow the server to validate the client's identity (making sure the client knows the required password) without actually transmitting the password itself. EAP extensions Paleker (2004) and Funk (2004) allow client and server mutual authentication, and also allow for confidentiality and integrity of the authentication information exchange.

Anti-virus: At the heart of any security architecture, there is a strong anti-virus product that includes automatic updates of definitions when the PC is connected to the server. This process must be automated, and should not require user intervention. One of the latest products should cover the application’s needs for virus protection. This is the responsibility of the principal investigator at each partner performing tests or evaluation.

Personal Firewall: A personal firewall product is a necessity for the modern road warrior.

Personal firewall products can be configured for dual-zone protection – leaving system access unrestricted while on the trusted local network, and providing tight security while on the untrusted Internet.

Encryption (either file/folder or full disc): It is the only way to ensure that the data remains secure, even if the device is not is to encrypt the data on the PC. A product that also offers e-mail encryption provides enhanced security.

Virtual Private Network (VPN): All connections between the mobile host and the corporate network should take place over a VPN. This ensures that the communication channel remains secure.

Access Control: Current design and implementation of the ADAS&ME application assumes that a specific user operates as the security administrator of his/her own data.

Physical Security: All the devices must be protected. This can be done by using hardware like locks and cables, or via software by using software products like Computrace, which, the moment the stolen computer is connected to a phone line or has access to the Internet, silently reports the PC's location to the Computrace Monitoring Centre.

During the pilot set-up the communication system shall be audited in order to validate security requirements. Hacking attacks shall be done in order to detect any security holes. The policies that are developed and the processes that are put in place to enforce them are only going to be effective if there are regular audits of the system. Monitoring of adherence to policy and investigation into non-compliance is required on a regular basis.

Understanding where the weaknesses in the system are, is the best way to find measures to correct them. Above all, polices and processes need to be reviewed and updated on a regular basis. Policy should never be considered static.

Information security is a difficult subject to address when the devices in question are safely tucked away behind the corporate firewall. Once they move outside the corporate firewall, managing those devices becomes much more difficult.

Summarising, concerning the security issues, the ADAS&ME system needs to:

- Identify the specific security requirements / threats / vulnerabilities associated to the various categories of users and data types.
- Study the related technology available.
- Define an appropriate security policy for accessing the information.
- Study the impact of adding security on the availability / performance of the system.
- Propose the conceptual structure and specific measures required to improve the security of the system.

This will be done during the project and in particular during the WP2.3 Risk Analysis and WP9.6 Security and privacy issues.

9 ANNEXES

Annex 1. ADAS&ME Ethics checklist

	Please circle as necessary	
Is there a need for ethical approval?	Yes	No
If yes, has it been approved?	Yes	No
Is the proposed research adequately designed, so that it will be of informational value?	Yes	No
Does the research pose risks of physical or psychological harm to participants by using deception, obtaining sensitive information or exposing them for risks in terms of safety and/or security hazards?	Yes	No
If risks exist, does the research adequately control these risks by including procedures, such as debriefing, removing or reducing risks of physical harm, or obtaining data anonymously? If that is not possible, will the research procedures guarantee that information will remain confidential?	Yes	No
Is there a provision for obtaining explicit and informed consent from all participants? Will the researcher provide sufficient information to potential participants so that they will be able to give their explicit and informed consent? Is there an explicit prior agreement in writing (the informed consent form) between the researcher and the potential participants? The explicit and informed consent should also make it clear that the participant is free to withdraw from the study at any time.	Yes	No
Will participants receive adequate feedback at the completion of the study, including a debriefing if that is necessary?	Yes	No
Do I as researcher accept my full responsibility for the ethical and safe treatment of all participants?	Yes	No
Have I as part of the project informed the Ethics Board about the ethical issues I have identified and of which I am aware?	Yes	No

Annex 2. Consent Form (templates)

Adaptive ADAS to support incapacitated drivers Mitigate Effectively risks through tailor made HMI under automation

This part will be filled by both participant and investigator.
Research participants' identity and dated signatures of the participant affirming that consent was given
The information shown below identifying the participant should be entered in the designated spaces at the time of execution of the consent document.
Name: _____
DoB: _____
Anonymisation Code:_____
Participant Consent Form
Title of the study:
Place of the study:

	Please circle as necessary	
I was informed about the effect to be expected, about possible advantages and disadvantages as well as about possible risks verbally and in writing by the test leader about the aim, course of the study.	Yes	No
I have read and understood the written information handed out for the study mentioned above. My questions in connection with the study have been answered satisfactorily. I can keep the written information and receive a copy of my written declaration of consent.	Yes	No
I had sufficient time to take my decision	Yes	No
In case an incident arises contrary to expectation an insurance consists for me in the legally specified scale. The insurance was constructed by ……. for this study.	Yes	No
I have spoken to: Dr./Mr./Ms.		
I understand that I am free to withdraw from the study at any time without having to give a reason for withdrawing and without affecting my future medical care	Yes	No
I agree to take part in the study?	Yes	No
The confidentiality of my personal data was assured to me.	Yes	No

Personal date will used anonymised at the publication of the studies results. I approve of the fact however under a strict compliance with the confidentiality that the responsible experts of the authorities and the ethic commission may take look for examining and control purposes in my original and anonymized data.		
I accept my face, voice, physiological bio-signals and driving behaviour parameters to be recorded and the information to be used in reports with no other personal information attached	Yes	No
If after effects appear, I will contact Dr./Mr./Ms.		

Signed .....

Date.....

Name (in block letters).....……

Investigators' confirming statement
I have given this research participant information on the study, which in my opinion is accurate and sufficient for the participant to understand fully the nature, risks and benefits of the study, and the rights of a research participant. There has been no coercion or undue influence. I have witnessed the signing of this document by the participant.
Investigator's Name: _____
Investigator's Signature:_____
Date: _____