

**INFORMATION SOCIETY TECHNOLOGIES (IST)
PROGRAMME**



Dangerous **Good** Transportation **Routing**, Monitoring and
Enforcement

GOOD ROUTE
IST-4-027873-STREP

GOOD ROUTE Ethics Manual			
Deliverable No.		D8.1	
Workpackage No.	WP8	Workpackage Title	Guidelines, Training and Standards
Activity No.	A8.4	Activity Title	Ethical and legal issues
Authors		Dr. Alex Bullinger, Marcel Delahaye (COAT), Maria Gemou (CERTH/HIT)	
Status (F: final; D: draft; RD: revised draft):		F	
File Name:		GOOD ROUTE-COAT-D-WP8-V3-GOOD ROUTE Ethics Manual.doc	
Project start date and duration		01 January 2006, 36 Months	

Table of Contents

TABLE OF CONTENTS	I
LIST OF TABLES	II
ABBREVIATION LIST	III
EXECUTIVE SUMMARY	IV
1. INTRODUCTION	1
2. PROJECT DESCRIPTION	3
3 GOOD ROUTE ETHICS ADVISORY BOARD	5
4 LEGISLATION RELEVANT TO GOOD ROUTE	7
4.1 GOOD ROUTE PILOT SITES LEGISLATION	7
4.1.1 <i>Swiss regulation</i>	7
4.1.2 <i>Italian regulation</i>	8
4.1.3 <i>Finnish regulation</i>	8
4.2 EU DIRECTIVES FOR TRANSPORTATION OF DANGEROUS GOODS	10
5 GOOD ROUTE ETHICAL POLICY CONCERNING SECURITY, PRIVACY AND TRANSPARENCY ISSUES	13
5.1 EU LEGISLATION ON ETHICAL ISSUES	13
5.2 INTERNATIONAL CONVENTIONS AND DECLARATIONS ON ETHICAL ISSUES	15
5.3 CONFIDENTIALITY/ PROTECTION OF PERSONAL DATA	16
5.4 INFORMED CONSENT.....	16
5.5 OTHER SECURITY ISSUES	20
5.6 RISK ASSESSMENT	25
6 GOOD ROUTE SPECIFIC ETHICAL ISSUES	27
6.1 ETHICAL ISSUES CONCERNING THE PROJECT OBJECTIVES	27
6.2 THE GOOD ROUTE COMMUNICATION, ENFORCEMENT MODULE AND UI FROM AN ETHICAL POINT OF VIEW	29
6.3 THE GOOD ROUTE DSS FROM AN ETHICAL POINT OF VIEW	29
6.4 ETHICAL ISSUES CONCERNING THE QUALIFICATION OF PILOT DRIVERS	30
7 CONCLUSIONS	31
REFERENCES	32
ANNEX I: TEMPLATE ON ETHICAL & LEGAL ISSUES	34
ANNEX II: GOOD ROUTE INFORMED CONSENT FORM TEMPLATE	41
ANNEX III: PIECES OF EU DIRECTIVES	45
DATA PROTECTION DIRECTIVE 95/46/EC	45
DIRECTIVE 97/66/EC ON DATA PROTECTION IN THE TELECOMMUNICATIONS SECTOR	52

List of Tables

Table 1: Overview of GOOD ROUTE Pilot sites..... 7
Table 2: Board for the Pilots monitoring according to the GOOD ROUTE Ethical Policy. 20
Table 3: GOOD ROUTE objectives vs. main ethical issues..... 28

Abbreviation List

Abbreviation	Term Description
ADR	Agreement concerning the international carriage of Dangerous goods by Road
BLEVE	Boiling Liquid Expanding Vapor Explosion
CPU	Central Processing Unit
DG	Dangerous Goods
DSS	Decision Support System
EC	European Commission
HMI	Human Machine Interaction
I2I	Infrastructure to Infrastructure
I2V	Infrastructure to Vehicle
ISO	International Standards Organization
IT	Information Technology
PC	Personal Computer
RBS	Road Beacons Systems
RFID	Radio Frequency Identification
SSL	Secure Socket Layer
STREP	Specific Targeted Research Projects
TCP/IP	Transmission Control Protocol/ Internet Protocol
UI	User Interface
V2I	Vehicle to infrastructure
V2V	Vehicle to Vehicle
VCE	Vapor Cloud Explosion
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WP	Work Package

Executive Summary

The current Deliverable is prepared in the context of WP8 “Ethical and legal issues” of the GOOD ROUTE project and constitutes the GOOD ROUTE Ethics Manual.

All aspects that should be taken into consideration from the ethical and legal point of view, during the implementation and the testing of the GOOD ROUTE system are presented and correlated to the specific items of the project.

It will be of vital importance to ensure that ethical aspects will be applied, basically on the following three different levels:

1. data protection and respect of privacy especially for the **truck driver**.
2. high level of data security for dissemination of information about test subjects among the different **Consortium partners**.
3. **Rerouting algorithm**: different ethical principles for the calculation of a new route will be taken into consideration.

The authors of this manual regard the following quotes written in the DoW as mandatory for all Partners and the whole duration of the project. Maybe one of the most important clarifications in the DoW is about security issues:

“The demonstrator vehicles equipment should not directly affect the safety critical systems. This means that the tests on the road will be possible and not require a special permission and escort from the Police Authorities.”

Moreover, also in the DoW, it is stated that *“We assure that within GOOD ROUTE we will fully respect and promote the ethical principles that are guiding our research activity: We conform to the rights / ethical principles of human dignity, integrity of the person, democracy, prohibition of degrading treatment, cultural, religious and linguistic diversity, equality, freedom of expression and information, the freedom of research, consumer protection, the right of the child, the elderly and the handicapped, non discrimination, privacy, protection of personal genetic data, as they are described in the Charter of European Fundamental Rights. Our research is only performed for purposes of betterment of the lives of European citizens.”* and that *“All national legal and ethical requirements of the Member States where the research is performed will be fulfilled”*.

In accordance with these commitments written in the DoW, the mentioned ethical principles will be specified in this Deliverable. Special emphasis will be given to the ethical evaluation of the planned pilots and the rerouting algorithm.

1. Introduction

The current document constitutes the GOOD ROUTE project Ethics Manual. It defines the ethical code of research conducted within GOOD ROUTE. All key ethical and legal issues implicated with the project Pilot plans and in general with all activities of the project have been identified in this document. Furthermore the respective project policy towards the monitoring and control of relevant emerging issues has been established.

All project Partners' research, dissemination and testing activities will be scanned on the basis of the information listed in this manual. Relevant national and international European conventions, are fully integrated in the manual. Utilising a template on "ethical and legal issues" that has been distributed within the Consortium, specific national standards and local conventions of ethical committees have been detected and integrated in the Ethics Manual.

In general, this manual is conceptualised to offer guidelines for all research activities performed in the context of GOOD ROUTE. Monitoring of adherence to this manual will be done at the maximum possible degree, to create the required "ethical awareness" among the Partners.

Chapter 1 of this Deliverable introduces the objectives of this manual, Chapter 2 provides a short project description, Chapter 3 includes some information about the GOOD ROUTE Ethical Advisory Board, established to monitor the project processes from an ethical point of view. Chapter 4 provides the legal and ethical regulations and guidelines, applicable nationally and locally in each GOOD ROUTE Pilot site as well as the EU legislation that is related to Dangerous Goods transportation.

Chapter 5 presents the Ethical Policy of GOOD ROUTE concerning security, privacy and transparency issues. In this section, all guidelines that have to be followed according to the relevant national and international legislation to assure security in the implementation of the system and the data sharing are provided. All national and international Directives that are considered applicable have been outlined and their content is shortly described. Upon the guidelines of Chapter 5, Chapter 6, a view on the ethical issues arisen regarding some critical items of GOOD ROUTE, such as the overall objectives of the project, the enforcement module, the DSS and the drivers' qualifications is presented and the aspects that have to be taken into consideration for each of them are stressed out. Finally, in Chapter 7, the main conclusions are presented.

Annex I provides the template, by means of which, the legal and ethical policies of the Pilot sites have been collected, Annex II includes the Informed Consent form, that is discussed in Chapter 5 and should be distributed prior to the GOOD ROUTE Pilots. Finally, in Annex III, some pieces from the Directives, on which the current Ethics Manual has been based, are quoted.

2. Project description

GOOD ROUTE is a STREP, aiming to develop a co-operative system for dangerous goods vehicles routing, monitoring, re-routing (in case of need), enforcement and driver support. This objective will be based upon dynamic, real time data, in order to minimise the societal risks related to their movements, whereas still generating the most cost efficient solution for all actors involved in the logistic chain. New classification scheme of the dangerous goods (according to ADR) with infrastructure based safety measures, context of transportation (i.e. level of loading) and vehicle characteristics will also be performed, dynamic data collection and fusion will be made through I2V/V2V sources and a series of on-board sensors, risk calculation algorithms will be realised, leading to a new route guidance function, the “minimum risk route guidance”.

To achieve its goals, the project aims to develop:

- A classification system and ontological framework between dangerous cargo, vehicle types and road infrastructure elements, to automatically permit or re-route specific dangerous good vehicles through specific road infrastructure.
- A collaborative platform, that is able to gather and process in real time vehicle and cargo, as well as environmental data (road status, unexpected obstacles, weather conditions, population density), as input to an optimal routing and route guidance system.
- A minimum risk guidance system, that would be able to route and re-route dangerous goods vehicles, taking into account individual and societal risk (based upon the collaborative platform based dynamic data), as well as performing conflict resolution and equity schemes.
- A Control Center algorithm, to oversee the routing and monitoring of all dangerous goods vehicles within a certain geographical area, provide the necessary traffic and environmental data to them and inform in real time their logistic chain for any unscheduled re-routing required.
- An on-board automatic data retrieval and storage system, to monitor key dangerous goods vehicle parameters (actual vs planned route, speed, weight per axle, etc.), able to supply it to local nodes (i.e. police car at toll station or before tunnel/bridge, etc.), for enforcement purposes.
- Optimal user interfaces for both the drivers of the dangerous goods vehicle and the control operator, to provide them with appropriate information and/or warning, without causing them workload enhancement or other unnecessary behavioural adaptations.

The system will be integrated with an automatic, local node based, enforcement functionality and tested in 3 Pilots throughout Europe (in Finland, Switzerland and Italy), with emphasis in densely populated areas, tunnels and bridges. In addition, rerouting info and estimated delays will be communicated to the vehicles thus optimally combining safety with transportation efficiency enhancement.

Dangerous goods are defined as the substances that can have harmful effects for human, environment and property. The classification of Dangerous Goods follows the “**ADR, Agreement concerning the International Carriage of Dangerous Goods by Roads**” of 30th September 1957, that has been included in **the Annex E of the ECE rules 1172/98**, which has been reported by the EC Directive **200017/CE of the 29th January 2001**. The latest relevant

ADR is the ADR 2005, applicable as from **1 January 2005**. This will constitute the basis for the GOOD ROUTE relevant research activities.

These harmful effects of the dangerous goods exist due to their nature; the hazardous properties or the state of the above substances. Each day, products defined as dangerous goods, that are necessary for maintaining European's quality of life, are transported from one point to another within or throughout Europe. These transportations are too numerous to accurately record and are estimated in multi-millions per year. With this amount of movements, there is great potential for endangering human life and damaging the environment through accidents during transportation. For this reason many countries are currently providing regulations, in order to "handle" dangerous goods in terms of packing, loading, transport, unloading and unpacking. Still, such rules are not always based upon rational policies nor solve the problem. For example, by law today in Greece dangerous goods vehicles are not allowed to pass through certain new tunnels, the alternative roads, though, pass through densely populated areas, thus resulting still a high risk situation. One of the main reasons for not allowing such vehicles in general to go through specific infrastructure (i.e. tunnels, long bridges) is the lack of knowledge of the specific cargo of the vehicle (what it is, is it loaded or not, up to which level, etc.) and its properties in relation to the safety systems installed at the particular infrastructure. If such knowledge existed accurately and dynamically, the highest amount of dangerous goods vehicles could safely use the main roads and infrastructure elements.

The transportation of dangerous goods involves risks and has the potential to harm not only the truck's driver, but also the population being present at a certain distance along the pathway of the truck. The aforementioned population represents the off-road residents living along the pathway and the on-road drivers and passengers of vehicles moving near the ADR vehicles. The consequences of a road accident involving dangerous goods can be different types of fires (pool fire, flash fire and jet fire), explosions (vapor cloud explosion – VCE, boiling liquid expanding vapor explosion – BLEVE), and release and dispersion of toxic substances (toxic gas cloud).

The most important hazards during the transportation of dangerous goods are due to possible loss of containment. Release of flammable gases or vapors can end up to flash fire and VCE, while flammable liquids usually result in pool fires. Jet flame is another type of fire that can be provoked by immediate ignition of a flammable gas released during an accident. Also, the containment might undertake a BLEVE or other types of explosions. In conclusion, flammable liquids result in fires rather than explosions. Explosion hazards exist mostly in the cases where the transported substances are quite unstable. If the dangerous good is toxic, its release will form a toxic gas cloud. Toxic and corrosive substances can spread during a release just like liquids do.

Accident history has shown that the risks related to the transportation of dangerous goods can be of the same magnitude as those caused by fixed installations.

All aforementioned adequately justify why ethical issues are quite critical for this project, from its theoretical framework and especially concerning its Decision Support System and mainly the equity schemes that will be established.

3 GOOD ROUTE Ethics Advisory Board

Any organisation performing experimental work with human beings or animals must have an ethics control committee that must evaluate all the aspects defined in its respective manual (Ethics Manual) and formally approve the experimental procedures.

Thus, from the early beginning of the project, an **Ethics Advisory Board** has been established, having the mission to verify beforehand all assessment tools and protocols to be used within GOOD ROUTE Pilots as well as all procedures of the project, in order to assure that they are in compliance with all recommendations, as defined in the current Ethics Manual.

Three renowned experts in the field, chaired by an experienced ethics coach, constitute the project Ethics Advisory Board. Assistance by external experts is also foreseen, when needed. The Ethics Advisory Board has the main responsibility for implementing and managing the ethical and legal issues of all procedures in the project.

The Ethics Advisory Board was established, consisting of 3 members and chaired by Dr. A. Bullinger. The current members of the GOOD ROUTE Ethics Advisory Board are the following:

1. Prof. Dr. rer. nat. Jürgen Maes

University of the German Army Munich, Expert in Justice Psychology.

2. Prof. Dr. Ullrich Meise (external expert)

University Hospital Innsbruck, Prof. Dr. Ullrich Meise is an experienced Professor in Psychiatry at the University hospital of Innsbruck. Since many years he is also providing help to developmental regions in central Africa.

3. Dr. Alexander Bullinger

COAT-Basel, leader of relevant Ethics Advisory Boards in various other research projects, such as SENSATION (IST-507231), AWAKE (IST-2000-28062), AGILE (QLRT-2001-00118) and ISLANDS (QLRT-2001-01637).

In addition, an external expert's assistance is foreseen for the execution of the tasks of the GOOD ROUTE Ethics Advisory Board, which is namely **Prof. Dr. Thomas Penzel**, a very renowned and experienced sleep researcher at the University of Marburg in Germany.

The contact details of the GOOD ROUTE Ethics Advisory Board secretary are provided below:

COAT-Basel
Wilhelm-Klein-Str. 27
4025 Basel

Contact Person details

Marcel Delahaye
Tel. +41 (0) 61 325 54 86
Fax. + 41 (0) 61 383 28 18

E-Mail: key@coat-basel.com

4 Legislation relevant to GOOD ROUTE

4.1 GOOD ROUTE Pilot sites legislation

A major issue that should be taken into consideration during the GOOD ROUTE Pilots is the laws and standards that regulate the dangerous goods transportation in each GOOD ROUTE Pilot site. The Pilots, concerning the evaluation scenarios and the whole way of execution, have to be in absolute conformity with the national and local regulation in each case.

There are three Pilot sites in GOOD ROUTE, a short overview of which is provided in the following table:

No	Resp. partner	Other (and/or external) involved partners	Location	Dates
1	North: FINRE (Finland)	SKAL (finnish transport and logistics), IVECO	Turku – Helsinki	Month 30-32
2	Central: Gotthard Road Tunnel (Switzerland)	COAT, IVECO	Crossing from Italy to Switzerland	Month 28-30
3	South: SITAF (Italy)	CRF, IVECO	Turin district	Month 26-28

Table 1: Overview of GOOD ROUTE Pilot sites.

In the following sections, the national regulation concerning the dangerous goods transportation in the country of each GOOD ROUTE Pilot site is provided. For the collection of the data, presented in the following sections, a questionnaire on ethical and legal issues (see Annex I) was distributed and was filled in by all Pilot sites.

This template can be also used as a sort of preliminary checklist for the Pilot conductor, before proceeding with any experiment.

4.1.1 Swiss regulation

Different guidelines and standards exist in Switzerland for the road transportation of dangerous goods. The federal bureau for roads (ASTRA) is the main body responsible for the road transportation regulation in Switzerland. In general Swiss law is in accordance with the European guidelines. Transportation within Switzerland as well as cross-border transportation is based on the “Agreement concerning the international carriage of Dangerous goods by Road (ADR)”. Swiss legislation itself is regulated in the ordinance of “transportation of dangerous goods on the road” (SDR) and the ordinance of “dangerous goods delegation (Gefahrgutbeauftragtenverordnung -GGBV)”. SDR is based on ADR and includes further special provisions, exceptions and deviations.

In addition, according to the GGBV, each enterprise of any nature that transports, delivers or receives dangerous goods is obliged to appoint and to instruct a dangerous goods delegate.

Finally, the “Weisung für Arbeit im GST” arrangement includes all relevant regulations for the work tasks performance within the Gotthard road tunnel.

In consequence of the fire catastrophe in the Gotthardtunnel, on the 24th of October, 2001 (11 people died, the most severe accident in the tunnel history) new safety requirements were implemented; for example the dose system and the drop meter system were invented to control the passages of the trucks in the mean traffic time.

Another relevant regulation is the one, titled “Flyer for safety and optimal traffic flow in road tunnel”: With the start of the summer holiday season, the Swiss Federal Roads Authority has released a flyer, aimed at optimising road safety and traffic flow in tunnels. It explains in simple terms and in three languages, what road users can do to keep traffic flow at smooth levels, and how they should behave in the event of a traffic jam or a fire inside a tunnel. The flyer is handed out to drivers of transit vehicles at the country’s main border crossings, and when traffic jams occurs on the Gotthard route.

All national and local regulation relevant to the dangerous goods transportation can be found at: www.gotthard-strassentunnel.ch.

More information about the regulations for dangerous goods transportation in Switzerland can be found at the following web pages:

- <http://www.astra.admin.ch/html/de/news/gefahrengut/index.php> (in German).
- <http://www.astra.admin.ch/html/it/news/gefahrengut/index.php> (in Italian).
- <http://www.astra.admin.ch/html/fr/news/gefahrengut/index.php> (in French).

"Anhang 2 der SDR / Appendice 2 SDR", where details about allowed goods and quantities in the tunnels are listed, is also important for the Gotthard Road Tunnel and should be taken into consideration. Following the link "Anhörung vom 24. Juli 2006 / Consultazione dell 24 luglio 2006", the draft of the new regulation being valid from 2007 can be found.

4.1.2 Italian regulation

All the transport of dangerous goods in Italy is regulated by the ADR.

The areas that the DG vehicles drivers are allowed to travel through, except from the urban regions, normally the transit is also allowed in the national roads and the motorways and through all tunnels, bridges and other special infrastructure sites. The Highway Code’s articles that refer to the specific regulation in Italy in reference to the European regulation are the following:

- Article 168
- Article 315
- Article 366
- Article 367
- Article 368
- Article 369
- Article 370

4.1.3 Finnish regulation

The transportation of dangerous goods is in full compliance with the ADR legislation and no additional licence/application is needed. If the dangerous goods vehicle contains radioactive material, a special license is needed from the Radiation and Nuclear Safety Authority of Finland. Also, special transports (e.g. wide & long) must apply for licence from road authority.

Infrastructure managers and authorities do not monitor the routes DG transports. The only monitoring action is performed in terms of the logistics of the transportation companies (which differ from each other).

General guidelines, standards and regulations for the road transportation of dangerous goods in Europe can be found at the following web sites (Directorate-General Energy and Transport):

- http://europa.eu.int/comm/dgs/energy_transport/security/goods/index_en.htm
- http://ec.europa.eu/dgs/energy_transport/security/goods/legislation_en.htm

The Finnish Ministry of Transportation and Communications is responsible for the drafting of guidelines concerning the transport of dangerous goods in Finland. The main act governing the transport of dangerous goods in Finland is the *VAK Act* of 1994. It sets out the main provisions for the general transport of dangerous goods by each transport medium, i.e. by Road, by Sea, by Air, etc. Each specific transport medium has its own governmental decree. Hence the transport of dangerous goods by road is covered by the “Government Decree on the Transport of Dangerous Goods by Road”.

This Decree applies to the transport of dangerous goods by road when the transport starts, takes place and ends in Finland. Should the transport of dangerous goods start, take place or end elsewhere than in Finland, the transport of dangerous goods by road in Finland is governed either by the “Government Decree on the Transport of Dangerous Goods by Road” or by the European Agreement concerning the “International Carriage of Dangerous Goods by Road (ADR)”.

This Decree however is specific to the transport of goods by road any other transport medium used in the transport of one particular item (say a container shipped from Sweden to Finland, driven by road to the railway and transported by rail to Russia) must comply with each specific governmental decree regarding each transport medium.

The Government Decree on the Transport of Dangerous Goods by Road begins by classifying what are dangerous goods. Next it outlines the roles and responsibilities of all parties concerned in relation to the transport of dangerous goods, i.e. consignor, consignee, carrier, driver, etc. The training of personnel involved with the transport of dangerous goods is carried out in accordance with the *VAK Act* (drivers of dangerous goods vehicles must have an ADR license).

The Decree also outlines the regulations with regard to the construction, approval and technical requirements of dangerous goods vehicles, tanks and containers. Finland recognises measures to prove conformity of dangerous goods tanks and containers in accordance with European Directive 1999/36/EC, with the exception of the material of a tank and its accessories belonging to transportable pressure equipment, which shall be resistant to brittle fracture up to -40°C.

The Decree states that the police shall supervise the transport of dangerous goods by road within Finland. Transport of dangerous goods by road from and to Finland shall be supervised by the Customs Administration and the Border Guard. Transport operations by the Defence Forces are governed by the *VAK Act*. The Radiation and Nuclear Safety Authority (STUK) in Finland shall act as supervisor of the transport of radioactive materials in co-operation with the police. Inspections of dangerous goods vehicles, tanks and containers are carried out by the relevant authority. These may be planned or random, and take place in specified testing areas.

More information on the regulations regarding transportation can be found at <http://www.mintc.fi/scripts/cgiip.exe/WService=lvm/cm/pub/showdoc.p?docid=2199&menuid=234>.

However, these provisions, with regard to transportation of dangerous goods, do not affect the GOOD ROUTE Pilots, since there will be no transportation of real dangerous goods cargo; it will be only simulated.

4.2 EU Directives for Transportation of dangerous goods

International transports of dangerous goods, in several modes, have been regulated by ADR, RID or ADN, which are based on international agreements. These agreements are frequently adjusted to the most recent technical and safety standards concerning transportation of dangerous goods and are introduced in specific EU Directives which are applicable also to national transport except from transport between the EU member states.

The EU Directives that refer to the regulation of the transportation of dangerous goods are outlined below.

- **Council Directive 94/55/EC** of 21 November 1994 on the transport of dangerous goods by road ("ADR framework directive").

The first directive about the land transport was Directive 94/55 known as the "ADR framework directive". The provisions of the ADR agreement are made uniformly applicable to road transport nationally and between Member States. It contains standards for the classification, packaging and labelling of dangerous substances as well as the state and construction of vehicles to transport them.

- **Council Directive 96/86/EC** adapting to technical progress Council Directive 94/55/EC.
- **Council Directive 99/47/EC** adapting for the second time to technical progress Council Directive 94/55/EC.
- **Council Directive 2001/7/EC** adapting for the third time to technical progress Council Directive 94/55/EC.
- **Council Directive 2003/28/EC** of 7 April 2003 adapting for the fourth time to technical progress Council Directive 94/55/EC.
- **Council Directive 2004/111/EC** of 9 December 2004 adapting for the fifth time to technical progress Council Directive 94/55/EC.
- **Council Directive 95/50/EC** of 6 October 1995 on uniform procedures for checks on the transport of dangerous goods by road.

This Directive provides a list of items to be checked and the issuing of a copy of the report on the road check carried out. This way any authorities can get the information carrying out a second road check in the same Member State or in another one.

- **Council Directive 2001/26/EC** of the European Parliament and of the Council of 7 May 2001 amending Council Directive 95/50/EC on uniform procedures for checks.
- **Council Directive 2004/112/EC** of 13 December 2004. adapting to technical progress Council Directive 95/50/EC on uniform procedures for checks.
- **Council Directive 96/35/EC** of 3 June 1996 on the appointment and vocational qualification of safety advisors for the transport of dangerous goods by road, rail and inland waterway.

In accordance to this Directive, "the activities including transport or the related loading or unloading of dangerous goods by road, rail or inland waterway", must appoint one or more safety advisors". As this definition includes loading and unloading activities, it is also appropriate to port undertakings which carry out these operations for the different forms of transport at land. The function of safety advisors exists therein to help prevent risks which these activities involve to those carrying out the job and other persons of the environment. The work of the safety advisor may be done by a person outside the enterprise or by an employee already busy on other tasks. The Commission underlines the importance of this directive regarding the importance of the human aspect in risks of accidents and the safety adviser function.

- **Council Directive 2000/18/EC** of the European Parliament and of the Council of 17 April 2000 on minimum examination requirements for safety advisers for the transport of dangerous goods by road, rail or inland waterway.

By this Directive, Member States shall take all required arrangements to assure that the safety advisers for the transport of dangerous goods are best instructed.

- **Directive 98/91** of the European Parliament and of the Council, relating to motor vehicles and their trailers intended for the transport of dangerous goods by road, and amending Directive 70/156/EEC relating to the type-approval of motor vehicles and their trailers (OJ L11 of 16 January 1999).

This Directive rules the allowance of category- of motor vehicles to carry dangerous goods. It implicates the technical requests in accordance to the ADR agreement and includes the provision of an EU certificate to facilitate the vehicle registration within the Member States.

- **Council Directive 1999/36/EC** on transportable pressure equipment.

With regard to the global aim to improve safety in transport, the European Union has released in 1999 the Directive 1999/36/EC to improve safety concerning transportable pressure equipment for the inland transport of dangerous goods by road and by rail. Under this directive are treated the receptacles and tanks used to convey Class 2 gases. The proposal aims to establish a system of EU conformity markings for new equipment and for periodic inspections, with the intention to free transport and use, including refilling, within the European Union. Directive 1999/36/EC is normally used to as TPED (Transportable Pressure Equipment Directive). For the purpose to disburden the use of the Directive, the Commission and Member States' experts has elaborated TPED Guidelines.

- **Council Directive 2001/2/EC** of 4 January 2001 adapting to technical progress Council Directive 1999/36/EC on transportable pressure equipment
- **Council Directive 2002/50/EC** of 6 June 2002 adapting to technical progress Council Directive 1999/36/EC on transportable pressure equipment.

In addition to the European law, there are also UN Recommendations on the transport of dangerous goods (http://www.unece.org/trans/danger/publi/unrec/rev13/13nature_e.html). The UN recommendations regarding the transport of dangerous goods can be found in the

form of "Model Regulations on the Transport of Dangerous Goods". Between other aspects, the Model Regulations cover principles of classification and definition of classes, listing of principal dangerous goods, general packing requirements, testing procedures, marking, labelling or placarding, and transport documents. These UN recommendations supplement the international guidelines of the ADR and national determinations.

5 GOOD ROUTE ethical policy concerning security, privacy and transparency issues

In this Chapter, the GOOD ROUTE ethical policy related to the security, confidentiality and transparency issues for the data gathering processes and the general system operation within GOOD ROUTE is provided, in compliance with all relevant laws, conventions, regulations and guidelines that are considered as most relevant.

5.1 EU Legislation on ethical issues

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 GOOD ROUTE. 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 need 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:

- **Charter of Fundamental Rights of the European Union (2001).** It is the most recent achievement of the European Union in the field of fundamental rights. Of course, this effort had to face different legal cultures and political constraints. Thus, the Charter constitutes the common denominator of the legal cultures of the Member States, the international conventions to which the Member States are member and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights. For reasons relating to the tasks and powers of the European Union the Charter is solely a "solemn proclamation" and is not legally binding. It has rather a declaratory function and could be the first step towards to legally binding regulations providing that the Union will choose for a closer political co-operation. The Charter of Fundamental Rights is addressed to the institutions and bodies of the Union and the Member States only when they are implementing Union Law (art. 51). The scope of the protected rights shall not exceed the level of protection and the meaning of corresponding rights set out either in the Community Treaties or the Treaty on the European Union (e.g. the freedom of establishment) or the European Convention for the Protection of Human Rights (art. 52). This practically means that the meaning, scope and limitations relating, for instance, to the protection of private and family life according to the EHRC (art. 8) and the Charter of Fundamental Rights (art. 7) shall be identical. Nevertheless, the Charter of Fundamental Rights in the course of the respective legal trend dedicates a separate article to the protection of personal data. Article 8 sets out the right to the protection of personal data of an individual and thus the protection of personal data has now an own legal basis apart from the right to respect for an individual's private life and the protection of the human dignity. Art. 8 of the Charter sets out the rules for the legitimate processing of personal data, notably that the processing shall be fair and for pre-specified purposes

¹ <http://wordnet.princeton.edu/perl/webwn?s=ethics>

² www.science.psu.edu/alert/frontiers/Glossary1-2001.htm

based on the consent of the data subject or other legitimate basis laid down by law. Reference is furthermore made to two rights of the data subject: the right of access to the data and the right to have it rectified. Finally, Art. 8 sets out the need for an independent authority which shall control the compliance with the data protection rules.

- **Directive 95/46/EC** (Annex III) of the European Parliament and of 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 (see Annex III of this document). OECD of Directive 95/46/EC is actively participating in the issues regarding the data protection, the data protection on the Internet as well as the protection of consumer rights with regard to e-commerce. First, OECD issued Guidelines governing the protection of privacy stipulating the fundamental principles (OECD, 1980). In 1998, OECD issued a Recommendation with regard to the implementation of the aforementioned Guidelines on global networks. The Recommendation addresses mainly commercial sites offering various goods and services, such as tourism, air travel ticket sales, finance etc. It is not legally binding unless the Internet service providers stipulate this explicitly. The Recommendation imposes the obligation to the web-site provider to refer with a hyperlink to the national legislation on data protection and the national Data Protection Authority. Moreover, every Data Protection Authority should be present on the Internet through relevant, well-documented and interactive sites. The web-sites shall also maintain on-line private statements giving details on the kind of data collected, the purpose of, the use of the clickstream data and processing to which they are subject, as well as the opportunity to opt out. In case of on-line payments by cards they should configure their systems in such a way that they ask for the card details once, provided that they store this information in highly secure files on non-networked computers. Warning messages on the risks of the Internet shall be provided in case of processing of confidential data. For confidential data the highest degree of security shall be implemented. The implementation of privacy enhancing technologies is also required. Moreover, web-sites should formally state the acceptance of full responsibility for the security and confidentiality of the personal data collected and processed. With regard to data subjects rights the Recommendation highlights the right to access on-line the information collected and stored directly or indirectly, i.e. clickstreams or purchased profiles.
- **Directive 97/66/EC** (Annex III) applies to data processed in connection with the provision of telecommunication services in public telecommunications networks, in particular via ISDN and public digital mobile networks, and is aiming to protect the privacy right of natural persons, as well as the legitimate interests of legal entities. Non-publicly available. The overriding aim of the Directive is to take account of technological changes and to make the provisions as technology-neutral as possible. In the preamble is stated that this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Article 5 states that Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised.
- **Directive 2002/58/EC** concerning the processing of personal data and the protection of privacy in the electronic communications sector.

- **Council Directive 83/570/EEC** of 26 October 1983 amending Directives 65/65/EEC, 75/318/EEC and 75/319/EEC on the approximation laid down by law, regulation or administrative action relating to proprietary medicinal products.
- **Directive 99/5/EC** on Radio Equipment, Telecommunications Terminal Equipment and the Mutual Recognition of Their Conformity. Access to control devices and control is a key issue from the viewpoint of the person.
- **Directive 2001/95/EEC**, which includes the general safety requirements for manufactures and distributors. The manufacturers must put on the market products that comply with the general safety requirements. They must also provide consumers with necessary information.
- **Low Voltage Directive (LVD) 73/23/EEC**, which aims to ensure that electrical equipment within certain voltage limits provides a high level of protection.
- **European Human Rights Convention (EHRC, 1950)**, with regard to automatic processing of personal data. It lays down the basic principles of a lawful data processing addressing the threats from the invasion of information systems, such as the data aggregation, at that time. In this respect, it concerns the *automatic* data processing, although the Member Countries could extend its applicability to non-automatic data processing. The Convention is of limited importance for EU countries after the enactment of the EC Directives on data protection.
- **Council of Europe (1999)**. It has adopted the Recommendation (99) 5 on the Guidelines for the protection of privacy in the information highways. These Guidelines may be incorporated in or annexed to codes of conduct of Internet service provider to obtain legal validity. The Recommendation is in line with the EC Data Protection Directives regarding the principles of the lawful data processing, the duties of the Internet service providers and the rights of the data subject. The Recommendation encompasses a series of detailed information what the users and service providers shall do to reduce the risks arising from the Internet. It is worth mentioned that the users are required to use digital signature and encryption techniques. On the other hand, the service providers are required to use certified privacy enhancing technologies, to ensure data confidentiality and integrity as well as logical and physical security of the network and the services provided over the network. The service providers shall also incorporate detailed privacy statements on the web-sites. Finally, the communication of sensitive data, for instance medical data, for marketing purposes requires the previous, informed and explicit consent of the data subject.

The information, guidelines and Directives concerning ethical issues provided by the EU for the scientific research is multifaceted; an overview can be found at http://europa.eu.int/comm/research/science-society/page_en.cfm?id=2995. The primary concerns of these Ethical guidelines go around medical, human and genetic research. However there are also guidelines, relevant to GOOD ROUTE (e.g. guidelines relating to personal data handling).

5.2 International conventions and declarations on ethical issues

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

- **Helsinki Declaration**, lastly amended in Tokyo 2004.

- **Convention of the Council of Europe on Human Rights and Biomedicine** signed in Oviedo on 4 April 1997, and the Additional Protocol on the Prohibition of Cloning Human Beings signed in Paris on 12 January 1998.
- **UN Convention on the Rights of the Child**, 2002.
- **Universal Declaration on the human genome and human rights adopted by UNESCO**, 1997.

The view of the **European Group of Advisers on the Ethical Implications of Biotechnology** (1991 -1997) and the **European Group on Ethics in Science and New technologies** (as from 1998) have been also taken into consideration.

Finally, the World Medical Association specified guidelines for medical research can be applied to GOOD ROUTE, even though the applications are technical and social rather than medical. These suggestions must be seen in addition, even though they are not specifically referred to the 6th Framework Programme. The main ethical considerations for medical research are the Scientific Merit, the Social Value, the Risks and Benefits, the Informed Consent, the Confidentiality and the Honest reporting of results.³

5.3 Confidentiality/ Protection of personal data

In GOOD ROUTE, all data that will be stored in the databases for the needs of the DSS and the algorithms are not considered personal, since these are related to professional drivers, which will be asked to participate in the Pilots, within the framework of their foreseen tasks. However, all other data, dealing with events taking place during the transportation, such as detection whether the driver has smoked or has consumed alcohol, etc. are not an objective of the GOOD ROUTE system; thus no relevant ethical issue is considered. The system platform will be open and it will be possible to be enriched with the monitoring and communication of other info, like those, but not in terms of GOOD ROUTE realisation. Thus, there is no need for a specific consent for such driver related data sharing in GOOD ROUTE.

5.4 Informed consent

The right of each individual according to Article 5c of the UNESCO Declaration to decide whether or not to be informed of the results of any medical, physical or genetic examination and the resulting consequences, if any, will be respected in full in terms of the GOOD ROUTE project.

Benefits derived throughout research within GOOD ROUTE, will be made available to the public, with due regard for the dignity and human rights of each individual and insofar as none of the aforementioned ethical issues are violated.

Every volunteer participating in the GOOD ROUTE project, actually in the GOOD ROUTE Pilots, needs to be fully aware of what s/he has been asked to do. Informed consent is the process by which a participant will be fully informed about the research in which he/she is

³<http://www.wma.net/e/ethicsunit/resources.htm>

going to participate. It originates from the legal and ethical right 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 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 informed consent elements is possible, namely the information given, the capacity to understand it and the voluntariness of any decision taken.

Respect for persons requires that participants, to the degree they are capable of, will be given the opportunity to choose what shall or shall 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, as lastly amended in Tokyo, 2004, and the Convention of the Council of Europe on Human Rights and Biomedicine (1997).

Whether a person has the capacity to understand the information depends on the ability to comprehend the nature and purpose of any course of action and the short and long-term risks and benefits of what is proposed.

Informed Consent is crucial in all aspects of social research and particular attention is given when disabled people are involved. However, this is not a current concern, since in GOOD ROUTE, only professional drivers will participate in the Pilots and in any other experiment (which can not be disabled by law). Thus, there will be no subjects, being unable to give a valid consent.

Information that will affect the respondent's willingness to participate will always be provided in appropriate accessible formats and never be deliberately withheld. Potential participants will also not be overwhelmed with unnecessary information. However it has to be monitored that drivers who are afraid of using the new technology have the right to withdraw and will not be forced.

In all cases, the prior, free and informed consent of the person concerned will be obtained (according to Article 5b of the UNESCO Declaration). If the respective participant is not in a position to consent, s/he will be excluded from any Pilots of the project. So it will be strictly monitored, that within the context of the GOOD ROUTE research and Pilot activities, none of the Partners involved will obtain consent or authorization for participants not being able to give this consent for themselves from a relative, legal counsellor or legal guide. Adherence to this regulation is mandatory, even if such an indirect consent would be guided by the person's best interest and be allowed under the respective national and European laws.

Especially during the Pilots, it should be monitored by the involved Partners that none of the drivers will be forced to test the new system if s/he feels uncomfortable. Of course, the same is valid for all other users of the system (control centre operators, logistics companies, etc.). However, the role of the truck drivers in the Pilots is more critical; thus these guidelines refer mainly to them.

All Pilot or experiments conductors within GOOD ROUTE will seek for the participants informed consent. Only under circumstances that provide the prospective participant sufficient opportunity to consider whether or not to participate and that the possibility of coercion or undue influence will be minimized, the candidate is allowed to take part. The information that is given to the participant or the representative will be in a language understandable to the participant or the representative. No informed consent, whether oral or written, may include any exculpatory language through which the participant or the representative is made to waive or appear to waive any of the participant's legal rights, or releases or appears to release the investigator, the sponsor, the institution or its agents from liability for negligence. In seeking informed consent according to the American Psychological Association (2002), the following information shall be provided to each participant:

1. the purpose of the research, expected duration, and procedures;
2. the possible risks, discomfort, adverse effects, and side-effects (if any);
3. a description of any benefits to the participant or to others which may reasonably be expected from the research;
4. explanations on confidentiality (and limits) of the data;
5. their right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing;
6. whom to contact for questions about the research and research participants rights.

In addition, appropriate insurance or indemnity to cover the participant in trial should be also provided.

When appropriate, one or more of the following elements of information shall also be provided to each participant:

- (1) a statement that the particular procedure may involve risks to the participant (or to the embryo or fetus, if the participant is or may become pregnant) which are currently unforeseeable (this case is very unlikely within GOOD ROUTE);
- (2) anticipated circumstances under which the participant's participation may be terminated by the supervisor without regard to the participant's consent;
- (3) any additional costs to the participant that may result from participation in the research (not expected to be the case within GOOD ROUTE);
- (4) the consequences of a participant's decision to withdraw from the research and procedures for orderly termination of participation by the participant;
- (5) a statement that significant new findings developed during the course of the research which may relate to the participant's willingness to continue participation will be provided to the participant; and
- (6) the approximate number of participants involved in the study.

However, within GOOD ROUTE, the aforementioned are slightly applicable, since the drivers that will participate in the Pilots will be professionals and there is no possibility that they will be not able to provide their informed consent or they will feel uncomfortable participating in the Pilots, since the systems' testing is foreseen in the context of their daily tasks. From this aspect, it may be the case that informed consent is normally not necessary for GOOD ROUTE; however, it is currently foreseen.

The following comments advise the supervisors/conductors of the Pilots and all other experiments with subjects how to provide information to prospective participants and therefore obtain consent:

- Informed consent is a **process**, not just a form. Information should be presented to enable persons to voluntarily decide whether or not to participate at 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, experimental 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 is 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. If payment is given to defray the incurred expense for participation, it must not be coercive in amount or method of distribution (not the case in GOOD ROUTE).
- The participants are told the extent to which their **personally identifiable private information** will be held in confidence.
- If **research-related injury** (i.e. physical, psychological, social, financial, or otherwise) is possible in research 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 GOOD ROUTE as the technical devices will not influence users' safety).
- **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.
- The participation is **voluntary** and the participant has the **right to withdraw at any time**. 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 experiment.

It will be the responsibility of the Partner conducting the respective trial to ensure that all uses of data/samples are in accordance with the consent obtained from the participant.

Informed consent shall be documented by the use of a written consent form approved by the GOOD ROUTE Ethics Advisory Board and signed by the participant. A copy shall be given to the person signing the form. The consent form shall be a written consent document that embodies the elements of informed consent required, as aforementioned. The relevant template is provided in Annex II of this document. Form 1 general information has to be filled in every case. The information concerning “INFORMATION ON THE RESEARCH STUDY” has to be provided to the participant, whenever considered appropriate by the Ethical Advisory Board.

In addition to the participant’s informed consent form, a supervisor’s confirming statement has to be filled in. The original will be given to the participant; a copy will be kept by the supervisor.

Finally, appropriate insurance or indemnity to cover the participant in a trial should be provided according to the regulations of the Local Ethics Research Committee (LREC). In any case, the GOOD ROUTE Ethics Advisory Board recommends insuring the participants. It should be stressed out that there will be no payment of participants for taking part in the research. Also no other form of inducement or material benefits for test subjects or their significant others will be granted. If an involved GOOD ROUTE Partner is ever in any doubt about a legal issue, he/she should refer it to its legal services and inform the GOOD ROUTE Ethical Advisory Board.

A board has been structured to guarantee that the GOOD ROUTE Pilots are performed according to the overall GOOD ROUTE Ethical Policy. A small workshop will take place before the GOOD ROUTE Pilots, to provide the identified Partners with relevant information about data protection and ethical issues interfering with the Pilots conduct.

The members and the responsibilities of the aforementioned Board are provided in the following table:

Partner	Responsible Person	Responsibility
CRF	Paola Bianconi	Overall responsibility for the monitoring of the Pilots.
GST	Marco Dotta	Swiss Pilot site responsible.
FINRE	Jussi Kiuru	Finnish Pilot site responsible.
SITAF	Caterina Ritta	Italian Pilot site responsible.
IVECO	Renzo Savio	Overall responsibility for the monitoring of the Pilots.

Table 2: Board for the Pilots monitoring according to the GOOD ROUTE Ethical Policy.

5.5 Other security issues

Besides the truck drivers personal data, integrity and confidentiality apply also for other types of information sharing foreseen in GOOD ROUTE (i.e. who should be allowed to see what and under which conditions). This applies for all channels of communication in GOOD

ROUTE; for example for the communication between the vehicle and the infrastructure, the vehicle and the control centre, etc. There will be data, related to the transportation routes as well as the company, that should not be, first of all, accessible from other systems and not foreseen actors (as these are defined by GOOD ROUTE). On the other hand, even the level of sharing of data between the involved actors *will be carefully examined by the A6.3 “Security and information reliability aspects”*, to assure that all security issues from all involved stakeholders point of view are taken into consideration. For example, the DSS will need to utilise some company data that should not be shared with other actors. All these levels of data sharing will be defined in A6.3 and will be finally reviewed by the GOOD ROUTE Ethical Advisory Board.

Finally, it is possible, that some of the information related to the drivers that will participate in the Pilots will be shared in terms of the results consolidation, and will be communicated among the Consortium Partners, so Pilot participants need to be made aware of this.

GOOD ROUTE 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 GOOD ROUTE 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 GOOD ROUTE 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. They create however new situations regarding security that should be dealt with in a thorough and convincing manner (Pangalos, 1997).

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 (Pangalos, 1997).

There are five steps that should be followed to assure the maximum possible security for GOOD ROUTE:

- 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 GOOD ROUTE.

- 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 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 GOOD ROUTE 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 GOOD ROUTE 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 GOOD ROUTE system is positively identified, both for the audit trail and for permission to access certain data.
- Availability, so that users can access the GOOD ROUTE 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 GOOD ROUTE 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 GOOD ROUTE 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 GOOD ROUTE system and services, will the threat to the system be reduced.

Once the policies are in place, a 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 GOOD ROUTE.

In the framework of GOOD ROUTE, 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.

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 GOOD ROUTE 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, policies 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 GOOD ROUTE 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.

5.6 Risk assessment

Thinking about risk assessment we have to consider two different layers: the participant level (driver, control centre operator, etc. level) and the general risk level in the transportation of dangerous goods for the population. The second one will be kept in boundaries by the quoted laws and aforementioned ethical suggestions. Regarding the participants in the GOOD ROUTE project, there are no direct risks, like, for example, in medical testing. The risks to the participant are more indirect. In general it is almost impossible to conceive a procedure, investigation, or process which would be without any risk. The importance of risk from the participant perspective should be considered as most important. In the process of "Informed Consent", risk and benefit should be outlined to the participant. Also his/her life/situation/personality may substantially influence the way in which a risk is perceived. The end point of the process consent will be given by the person to be part of the research project having considered all aspects of the process and asked all relevant questions. All relevant information will be given to the participants. This means that the project GOOD ROUTE will

be carefully explained, as described in the informed consent chapters. The choice that is made and the consent that is given will be without coercion or undue pressure being applied.

In conclusion:

- There will be no additional risk to human welfare by the GOOD ROUTE project. The cargo transported will be simulated; this means that no additional risk will be there in relation to this.
- No physical damage within the experiments will be taken in GOOD ROUTE. Any equipment connected to a participant will be evaluated for personal safety.
- Social inconveniences will be minimised (extremely limited traffic circulation caused by only one demo vehicle, respect of comfort and no hazard to local communities, etc.).

6 GOOD ROUTE specific ethical issues

According to the guidelines and the recommendations described in the previous Chapter, the most critical ethical aspects related with specific items (either systems or procedures) of the project are discussed in this Chapter.

6.1 Ethical Issues concerning the project objectives

The following table gives an overview of the GOOD ROUTE project objectives. Items that interfere with ethical issues, as described in Chapter 6, are in bold and underlined, whereas for each one of the objectives, the relevant ethical issues are outlined.

GOOD ROUTE objectives	Addressed Ethical Issues
<p><u>Critical analysis of dangerous goods</u> accidents, relevant localisation and practices, and the <u>needs of all actors</u> involved in dangerous goods transportation (dangerous goods companies, transporters, drivers, recipient clients, transport infrastructure owners, authorities, etc.), to specify an integrated, <u>cost-efficient</u>, law-abiding, <u>fair</u> and modular system.</p>	Data management, Privacy, Security
<p><u>Development of a classification</u> system and ontological framework between dangerous cargo, vehicle types and road infrastructure elements, to <u>automatically permit</u> or re-route specific dangerous good vehicles through specific road infrastructures (i.e. tunnels, long bridges, etc.).</p>	Delegation of control, Confidentiality
<p>Development of a <u>collaborative</u> platform, that is able to gather and process in real time vehicle and cargo as well as environmental data (road status, unexpected obstacles, weather conditions, population density) as input to an optimal routing and route guidance system.</p>	Data management, Privacy/ Security, Confidentiality
<p>Development of a <u>minimum risk guidance</u> system (WP2), that is able to route and re-route dangerous goods vehicles, taking into account individual and societal risk (based upon the collaborative platform based dynamic data), as well as conflict resolution and equity schemes.</p>	Road safety/Security
<p>Develop a Control Centre algorithm, to oversee the routing and <u>monitoring</u> of all dangerous goods vehicles within a certain geographical area, <u>provide</u> the necessary traffic and environmental <u>data to them and inform in real time</u> their logistic chain for</p>	Data management/Protection/Security, Privacy , Confidentiality

GOOD ROUTE objectives	Addressed Ethical Issues
any unscheduled re-routing required.	
Develop an on-board automatic data retrieval and storage system , to monitor key dangerous goods vehicle parameters (actual vs. planned route, speed, weight per axle, etc.), able to supply it to local nodes (i.e. police car at toll station or before tunnel/bridge, etc.), for enforcement purposes.	Data management/ Protection/ Security, Privacy, Confidentiality
Develop optimal user interfaces for both the drivers of the dangerous goods vehicle and the control operator, to provide them with appropriate information and/or warning, without causing them workload enhancement or other unnecessary behavioural adaptations .	Road safety
Integrate all functions on top of a vehicle prototype and test them in 3 Pilot sites, Europewide, to evaluate their reliability, usability, successfulness, cost-efficiency and thus estimate their potential safety impact and viability .	Product safety, Security
GOOD ROUTE will develop a communication infrastructure for cooperative information retrieval and exchange... thus making vehicles (trucks) not only system clients but also data and information providers (trucks and driver logs).	Data management/ Protection/ Security, Privacy, Confidentiality

Table 3: GOOD ROUTE objectives vs. main ethical issues.

According to the GOOD ROUTE DoW, each enterprise will send in real time, four different log files about each specific transport of dangerous goods:

- Driver log (e.g. training record, accident record, etc., in agreement with legislation about personal data).
- Vehicle log (tyres condition, age, total km, etc.).
- Material log (hazardous properties, transport conditions/ pressure/ temperature/ phase, quantity, etc.).
- Origin-Destination log (Origin, Destination, departure time, etc.).

The relevant European laws and Directives that should be taken into consideration for the above data flow for the reasons described in section 5.5 of this document are the following:

- Council Directive 83/570/EEC.
- Directive 98/44/EC.
- Low Voltage directive (LVD) 73/23/EEC.
- Charter of Fundamental Rights.

- World Medical Association Ethics.
- Directive 95/46/EC, Directive 2002/58/EC.
- World Medical Association Ethics.
- Directive 99/5/EC.

6.2 The GOOD ROUTE communication, enforcement module and UI from an ethical point of view

Regarding the data processing and information flow in the different communication types, Informed Consent, Privacy, Data protection, Data management, Biocompatibility and Confidentiality have to be fulfilled. Similar ethical guidelines have to be followed for the Enforcement module. If a driver is monitored via RBS or RFID, the selection of data that will be collected and sent to any entity has to be based on transparent procedures. Data ownership and privacy have to be fully respected. It has been stated that no private data of the drivers (history of past accidents, Criminal Records, medical history) will be neither collected nor sent to any entity. Stored or transferred data have to be on the highest technical security level. Whenever an experiment or study takes place, the participant has to be fully informed and aware of his rights (Informed Consent).

The relevant laws and directives are the following:

- Charter of Fundamental Rights.
- World Medical Association Ethics.
- Directive 95/46/EC, Directive 2002/58/EC.
- World Medical Association Ethics.
- Directive 99/5/EC.

In the same way, with respect to the safety of the driver using the HMI of the system, cognitive workload aspects have to be monitored. Informed Consent, Privacy, Data protection, Data management, Biocompatibility and Confidentiality are also applicable here.

The relevant laws and directives are the following:

- Council Directive 94/55/EC of 21 November 1994 on the transport of dangerous goods by road ("ADR framework directive").
- Charter of Fundamental Rights.
- World Medical Association Ethics.
- Directive 95/46/EC, Directive 2002/58/EC.
- World Medical Association Ethics.
- Directive 99/5/EC.

6.3 The GOOD ROUTE DSS from an ethical point of view

Another ethical issue that is raised within GOOD ROUTE is that one of the GOOD ROUTE Decision Support System and the risk analysis algorithm (taking into account the different social and business groups demands). The aim of the system is to propose a route with the minimum possible safety risk and the highest possible efficiency (also cost-efficiency).

However, the main issue that should be stressed out here is that the route proposed by the system may increase safety for the driver and the third parties; however it is difficult to fully achieve it. For example, the fact that a route that is proposed to the vehicle presupposes that it has not to travel through densely populated areas, but from regions with more limited population, which is indeed the less risky alternative for safety and environmental protection, still is a decision that may prove to be fatal for the selected region population and of course unethical.

Following just the common **Utilitarian principle** (act so as to produce the greatest amount of good for the greatest number, Mill 1863; in “Ethics Technology 2004”) does not lead to the best result. For example, enslaving 15 % of the population would probably due to a higher economic result but of course is absolute unethical. Transposing that to the re-routing system, it is obvious that if all dangerous goods vehicles were routed or re-routed to travel through a rural area with a low population density, it would be definitely unfair. So a **diversification of routes** is a necessity for the re-routing algorithm of the DSS. Perhaps, facts like the different population density during day and night may also be taken into account. For example a DG transport will cause less harm in front of a school after 6 p.m. than before.

Another major relevant ethical theory is **Kants’ categorical imperative** (in “Ethics Technology 2004), one acts on principles that could be willed to be universal law. One major suggestion by all philosophers to maintain the Kants’ categorical imperative is **publicity**. Publicity requires that everyone concerned must be aware of the principle you are using. Public workshops, open internet forums and press publications should be certainly envisaged to publish the GOOD ROUTE system functionalities, before the system is applied to the market.

In WP 2: “Minimum Risk Route Guidance System” different activities focus on a solution for a “fair” procedure for the decision module. In specific, special attention has to be paid to the equity schemes of A2.4 “Conflict resolution and equity schemes” that will be employed to rationalise the DSS decision process and will be closely monitored by the Ethical Advisory Board.

6.4 Ethical Issues concerning the qualification of Pilot drivers

The training standards for the professional drivers of DG vehicles are provided in Chapter 1.3 of ADR. With respect to the official ADR guidelines, people involved in the carriage of dangerous goods by road have to make sure that they and any of their employees who have any responsibility for such carriage are appropriately trained.

The persons that will participate in GOOD ROUTE Pilots have to be qualified, in order to assure that they will not cause any harm to third parties and the environment. Of course, this is done internally in the transportation companies and the validation of the qualifications of the drivers that will participate in the GOOD ROUTE Pilots is certainly not one of the objectives of GOOD ROUTE. However, in any case, the drivers that will be selected as subjects for the GOOD ROUTE Pilots will be professional truck drivers, and adequately qualified. They will be drivers or contractors coming either from CRF or IVECO and a copy of their certification will be made available, if needed.

7 Conclusions

All ethical aspects that should be taken into consideration in GOOD ROUTE, concerning its implementation, Pilot testing and dissemination activities have been presented in the current Ethics Manual.

The main issues have been the protection of personal data of the several users involved in the project during the implementation and the Pilots phase, the way all project trials should be performed and the issues that should be taken into account for the DSS algorithms, in order to conform to security, privacy and confidentiality guidelines.

All national and international guidelines, relevant to the Dangerous Goods transportation and the ethical issues arisen for GOOD ROUTE have been collected and outlined. Moreover, the specific regulations and legislation, valid in each Pilot site has been gathered through a template provided in Annex I and distributed to all Pilots conductors.

This Ethics Manual may be subject to changes, if it is considered appropriate and the responsible body for the monitoring of conformity to this is the Ethical Advisory Board of GOOD ROUTE, consisting of 3 members and an external expert and chaired by Dr. A. Bullinger (see Chapter 3 of this document). In addition, a Board responsible for the Pilots conduction, with regard to the conformity to all recommendation provided by this Ethics Manual, has been established and provided in section 5.4 of this document.

Summarising the guidelines of this manual, the GOOD ROUTE Consortium and its Ethical Advisory Board is committed to perform no experiments with persons unable to give a valid consent, which is not foreseen anyway, since all subjects will be professionals (truck drivers, control centre operators, etc.) and to share no personal information about them without their permission. The personal data will be strictly protected and unlinked anonymised (as much as possible). No genetic information will be collected. No user personal data and preferences will be sent around in the Network, nor will be available to any third party (i.e. for advertisement, marketing or even research – outside GOOD ROUTE objectives). Personal information should not be retained longer than 3 month after the end of the project.

As also explained, Pilot subjects activities such as drinking alcohol, smoking, etc. are not an objective of this project, thus all ethical issues related to that are not applicable in this case.

All Pilots participants will be requested to give their consent (although not necessary, since are professional drivers coming from the Consortium Partners) about participating in the Pilots and in any other activity of the project, after they have been respectively informed about the exact scope and the procedure to be followed. Finally, all algorithms that deal with decisions affecting third party and environment have to take into consideration the relevant ethical aspects, as outlined in Chapter 6 (in terms of the relevant WP of the project, and especially WP2).

References

- American Psychological Association (2002). Ethical Principles of Psychologists and Code of Conduct. *American Psychologist*, 57, 1060-1073.
- Charter of fundamental rights of the European Union. (2000) Nice.
- Committee of Ministers Council of Europe (1990). Recommendation (No. R(90)3).
- Council of Europe (1997). 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, Oviedo.
- Data Protection Working Party (2000). Privacy on the Internet – An integrated EU approach to On-line Data Protection, 5063/00/EN Final.
- Directive 2001/20/EC (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.
- Directive 97/66/EC of the European parliament and the council (1997). Concerning the processing of personal data and protecting of privacy in the telecommunications sector.
- Ethics & Technology 2004 by H. T. Tavanai. Ethical Issues in an Age of Information and Communication Technology. Wiley International Edition.
- Ethics in EU projects, Ethical issues in EU research proposals – checklist, updated 08.11.2005 in: http://europa.eu.int/comm/research/science-society/page_en.cfm?id=3205
- EU Directive 95/46/EC The data protection directive (1995).
- European human rights convention (1950)
- Freeman, L. & Peace, G. (2005) Information Ethics: Privacy and Intellectual Property. Information Science Publishing.
- Funk, P., Blake-Wilson, S., (2004) EAP Tunneled TLS Authentication Protocol Version 1, work in progress
- Johnson, D. H. & Sabourin, M. H. (2001). Universally accessible databases in the advancement of knowledge from psychological research. *International Journal of psychology*, 36, 212-220.
- Joseph, L. & Cook, D. (2005) in: Information Ethics: Privacy and Intellectual Property. Information Science Publishing. (p. 200)
- Knapp, S. & VandeCreek, L. (2003). A guide to the 2002 Revision of the American Psychological Association's Ethics Code. Professionell Resource Press, Sarasota Florida.
- Medial Research Council (2000). Personal information in medical research. In: Manual for Research Ethics. S. Eckstein (eds.). 367-390, University Press, Cambridge.
- Medical Research Council (1993). The ethical conduct of research on the mentally incapacitated, London.
- OECD (1980). Guidelines governing the protection of privacy and transborder flows of personal data.
- Palekar, A., et al. (2004), Protected EAP Protocol (PEAP), work in progress.
- Pangalos, G.: *Security Issues in a Mobile Computing Paradigm*, in Proc. of CMS'97, Communications and Multimedia Security, Vol.3, pp.60-76, 1997.
- Royal College of Psychiatrists (2000). Guidelines for Researchers and research Ethics Committees on Psychiatric Research involving Human Participants, Gaskell, London.
- Social Research Association (2003). Ethical Guidelines.
- World Medical association (2004). Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Participants, Tokyo.

Web sites

http://ec.europa.eu/dgs/energy_transport/security/goods/legislation_en.htm

http://europa.eu.int/comm/research/science-society/page_en.cfm?id=2995
<http://www.astra.admin.ch/html/de/news/gefahrengut/index.php>
<http://www.astra.admin.ch/html/it/news/gefahrengut/index.php>
<http://www.astra.admin.ch/html/fr/news/gefahrengut/index.php>
<http://www.gotthard-strassentunnel.ch>
<http://www.mintc.fi/scripts/cgiip.exe/WService=lvm/cm/pub/showdoc.p?docid=2199&menuid=234>
http://www.unece.org/trans/danger/publi/unrec/rev13/13nature_e.html

Annex I: Template on Ethical & Legal Issues

INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME



Dangerous Good Transportation Routing, Monitoring and
Enforcement

GOOD ROUTE IST-4-027873-STREP

Title	Ethical and Legal Issues template
Authors	A.Bullinger, M. Delahaye (COAT)
Summary	Aim of this template is to collect any local ethical and legal issues of the Pilot sites.
WP	8
Status	F
Distribution	Pilot conductors
Document ID	GOOD ROUTE-COAT-WP8. V1. Ethical and Legal Issues template.doc

1. At which level of organization, ethical controls are audited?

- laboratory or workgroup
- division or department
- institution
- regional
- national

2. Is there an international or national legislation, which you must follow when performing tests with human subjects?

- Yes
- No

If Yes, please give details (reference number and short description of procedure):

.....

.....

.....

.....

.....

.....

3. Is there an ethics controlling body in your country?

- Yes
- No

If Yes, please give details about the procedure:

.....

.....

.....

4. Is there an ethics controlling committee within your organisation?

- Yes
- No

If Yes, please give details about the procedure:

.....

.....

.....

5. Is there an established ethical control procedure which you must follow before performing tests with human subjects?

- Yes
- No

If Yes, please give a brief description of it:

.....

.....

.....

.....

.....
.....

6. Is there an established Data Protection Authority which you must follow before performing tests with human subjects and their personal data?

Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

7. Do you follow written procedures to protect privacy?

Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

8. Do you follow any official national or international guidelines on protecting privacy?

Yes No

If Yes, please give a brief outline and provide references.

.....
.....
.....
.....
.....

9. Do you clarify to the participants that all data collected in the activities they are participating is kept confidential and that their anonymity will be protected?

Yes No

If Yes, please give a brief outline and provide references.

.....

.....
.....
.....
.....
.....

10. Do you identify persons and their professions who are authorized to have access to the data collected?

- Yes No

If Yes, please give a brief outline and provide references.

.....
.....
.....
.....
.....

11. Will you provide information to the participants if you get aware of an illness

- Yes No

If Yes, please give a brief outline and provide references.

.....
.....
.....
.....
.....

12. Is every experiment evaluated for any biological or other effects?

- Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

13. Do you have written procedures for maintaining hygiene within your own group or institution?

- Yes No

If Yes, please give a brief outline of it:

.....

.....

If No, please explain the reasons briefly or what corrective actions you take?

.....

14. Do you have written procedures for safety of employees and volunteers within your own group or institution?

Yes No

If Yes, please give a brief outline of it:

.....

If No, please explain the reasons briefly or what corrective actions you take?

.....

15. Do you have procedures, facilities and expertise to test or verify equipment for patient safety to protect against electrical or magnetic hazards?

Yes No

If Yes, please give a brief outline of it:

.....

If No, please explain the reasons briefly or what corrective actions you take?

.....

16. Do you have procedures, facilities and expertise to test the patient safety of prototypes you develop?

Yes No

If Yes, please give a brief outline of it:

.....

.....

If No, please explain the reasons briefly or what corrective actions you take?

.....

17. Do you have procedures and expertise to verify bio-compatibility of the already existing test equipment which you will using during pilot testing?

Yes No

If Yes, please give a brief outline of it:

.....

If No, please explain the reasons briefly or what corrective actions you take?

.....

18. Is your organisation insured against risks as a result of breach of privacy, safety and bio-compatibility?

Yes No

If Yes, please give a brief outline of it:

.....

If No, please explain the reasons briefly or what corrective actions you take?

.....

19. For conducting results ethically and manage the risk, do you need to involve other organization (unit, division, department etc.) that also control and decide your research activity?

Yes No

If Yes, please give a brief outline of it:

.....

.....
.....
.....
.....
.....

20. What kind of experience do you have regarding the influence of the information flow on the mental workload of drivers?

Please give a brief outline of it:

.....
.....
.....

21. If applicable, please specify the shortcomings of the new routing and monitoring system (regarding possible risks), etc.:

.....
.....
.....

ANNEX II: GOOD ROUTE Informed consent form template

1. GENERAL INFORMATION

(This part will be pre-filled by the supervisor/conductor of each Pilot.)

The GOOD ROUTE Ethics Advisory Board reviewed this Pilot activity from the standpoint of the protection of human rights. The GOOD ROUTE Ethics Advisory Board found the study to be in compliance with the relevant regulations.

1.1 This version of the consent document was prepared on:

1.2 This trial was approved by the GOOD ROUTE Ethics Advisory Board on:

1.3 Names of the supervisors/conductors responsible for this project:

2. INFORMATION ON THE RESEARCH STUDY

(The following issues should be explained by each Pilot conductor/supervisor to the participant before the beginning of the trial.)

2.1 Title of the study

2.2 What is the purpose of this research study?

You are asked to take part in a research study under the direction of _____ . Other professional persons who work with him/her may assist or act for them.

These investigators are undertaking a research study to determine whether _____ . We expect to find _____ , which could lead to better methods of diagnosis / treatment / monitoring.

2.3 Who can take part in this study?

2.4 Why should I consider joining this study as a research participant?

2.5 Do I have to become a participant in this study? If I joined the study, can I change my mind and drop out before it ends?

2.6 What exactly will be done to me, and what kinds of treatments or procedures will I receive, if I agree to be a research participant in this study?

2.7 What kinds of harm can I experience in this study, and what will the investigators do to reduce the chances of harm?

2.8 What will the investigators do to make sure that the information they will collect on me will not get in the wrong hands?

2.9 What kinds of benefit can I expect personally from taking part in this study?

2.10 What kinds of benefit to others can come out of this study?

2.11 What will the investigators do, if I get injured in the study?

2.12 Will I get paid for taking part in this study?

2.13 Will I or my health insurance company be charged for any of the costs of this study?

2.14 Once I start in this study as a participant, what do I do if I want to find out more about the study, or to complain about the way I get treated?

2.15 Who gets to keep this document, once I sign it?

2.16 Which others may view or use the data of this document, if any?

3. DOCUMENTATION OF CONSENT

3.1 Research participant's identity

(This part will be filled in by the participant. The original will be kept by the conductor/supervisor; a copy will be given to the participant.)

Research participant's identity and the 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.

Participant's Name: _____

Participant's Birth Date: _____

Participant's Reference Number: _____

3.2 Participant Consent Form

*this part will be filled in by the participant.
The original will be kept by the investigator; a copy will be given to the participant.*

Title of the study:

Place of the study:

	Please circle as necessary	
I was informed about the effect to be expected, about possible disadvantages and about possible risks verbally and in writing by the test leader of the study.	Yes	No
I was informed about the purpose of research, the expected duration and the procedures verbally and in writing by the test leader of the study.	Yes	No
I was informed about the of any benefits to me or to others which may reasonably be expected from the research.	Yes	No
I was informed about the explanations on confidentiality (and limits) of the data.	Yes	No
I was informed about the right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing.	Yes	No
I was informed about whom to contact for questions about the research and research participants rights.	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 <ul style="list-style-type: none"> ◆ 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. Personal data will be used anonymised at the publication of the study's results. I approve of the fact however under a strict compliance with the confidentiality that the responsible experts of the authorities and the ethics commission may take a look for examining and control purposes of my original data.	Yes	No
If aftereffects appear, I will contact Dr./Mr./Ms. with the tel. no.		

Signed

Date.....

Name (in block letters).....

3.3 Investigators' confirming statement

(This part will be filled in by the conductor/supervisor. The original will be given to the participant; a copy will be kept by the conductor/supervisor.)

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: _____

3.4 Research participant's identity (participant unable to read the form; to be provided in an appropriate alternative media e.g. large print, audiotape, etc.).

(This part will be filled in by the participant. The original will be kept by the conductor/supervisor; a copy will be given to the participant.)

Research participant's identity and the 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.

Participant's Name: _____

Participant's Birth Date: _____

Participant's Reference Number: _____

Annex III: Pieces of EU Directives

Data Protection Directive 95/46/EC

In 1995, the EC Directive on the protection of personal data has been adopted by the Council. The Directive is the first attempt on EC level to recognise the right to privacy and harmonise the national laws. Some main characteristics of the Directive are that it applies equally to public and private bodies, to both automatic and non-automatic data processing, and that the protection is restricted to natural persons (as opposed to legal entities). Moreover, the data must form a part of a filing system, which is defined as any structured set of personal data accessible according to specific criteria.

- The Directive lays down following core principles / measures with regard to data processing:
- The fairness and lawfulness of data processing.
- The purpose limitation principle (data shall be processed only for pre-specified purposes and stored for no longer than this is necessary for the pre-specified purposes).
- The proportionality principle (data must be relevant and not excessive for the pre-specified purposes).
- The data quality (data must be accurate, kept up to date and where necessary erased or rectified).
- Transparency principle (data subject must have access to the data relating to him and the controller must provide the data subject with a series of information relating to the data processing).
- Voluntary participation of the data subject (data subject must give unambiguous and informed consent).
- Adequate security measures. (The data controller shall implement adequate technical and organisational measures to protect personal data from infringements related to data integrity, availability and confidentiality. The security measures shall comply with the state of the art and be appropriate to the nature of the data and the potential risks represented by the data processing. Moreover, the implementation costs is a key point).
- Data concerning the health of an individual are sensitive data and thus subject to specific rules allowing its processing. The Directive does not further specify the meaning of data concerning health.
- Where the processing is likely to present specific risks to the rights and freedoms of the data subject, for instance where sensitive data are processed for purposes other than the medical treatment, the processing is subject to prior checks by the national Data Protection Authorities.
- The implementation of specific and effective rules with regard to the liability of the person infringing the provisions of the Directive.
- The recognition of self-regulation instruments for the proper implementation of the purpose of the Directive in the various sectors. In this respect, codes of conduct of medical associations or chambers shall specify the general principles of the Directive tailored to the needs of each professional activity.

Article 2

For the purposes of this Directive:

(a) 'personal data' shall mean 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;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 8

Article 8 of the Directive on the processing of data related to health states that the processing of medical data shall be prohibited, unless

- the data subject has given his explicit consent (art. 8 par. 2 (a)) or
- this is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent (art. 8 par. 2 (c)), or
- the processing is necessary for the establishment, exercise or defense of legal claims (art. 8 par. 2 (e))

- the processing is required for the purposes of preventive medicine, medical diagnosis, treatment or for the management of healthcare services and where the processing is carried out by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (art. 8 par. 3).

Moreover, the Member States shall determine the conditions for the processing of identifiers of general application (art. 8 par. 7).

The Directive lays down a series of rights of the data subject, for instance the patient: These are:

- The right of access to his / her personal data.
- The right of erasure, blocking or rectification of the data which do not comply with the provisions of the Directive, are incomplete or inaccurate.
- The right to be informed of all relevant details relating to the data processing and the rights granted to him/her.
- The right to a judicial remedy for any breach of the above mentioned rights.

The first three aforementioned rights may be restricted if this is necessary for reasons relating to the protection of the data subject or the rights and freedoms of others or to prevent a criminal offence or for reasons relating to public security.

Article 29 (Data Protection Working Party: Working Document on Privacy on the Internet)

The Data Protection Working Party has been established by art. 29 of Directive 95/46/EC and is the independent advisory body on data protection and privacy. Its tasks are laid down in art. 30 of Directive 95/46/EC and in art. 14 of Directive 97/66/EC. The opinions and recommendations of the Working Party are not legally binding, reflect, however, the current trends on European level and influence the decisions taken by the European Commission and the Committee established by art. 31 of Directive 95/46/EC.

This working document seeks to raise awareness and to promote the public debate on issues of on-line data protection. It therefore provides detailed information on technical aspects of how the Internet and the communications through the Internet are organised and what are the main privacy risks arising from the use of the Internet. In this context, it aims at the same time to provide an interpretation of the data protection Directives in that field. It follows a "holistic" approach by basing the analysis of privacy risks, the obligations and rights of the involved parties on both the general data protection Directive 95/46/EC and the privacy and telecommunications Directive 97/66/EC.

The risks to privacy arise from the activities of the various intermediaries. For instance, the use of routers, e.g. the telecommunications nodes in the Internet, which have the characteristic that the information may pass through a non-EU country which may or may not have adequate data protection, if this at the time of transmission is the "shortest" way of transmission.

According to the opinion of the Working Party, Directive 97/66/EC applies to telecommunication service providers who connect Internet users and ISPs and access service providers who provide the requested Internet service, transfer the request from the Internet user to proxy server and then to the requested website. It also applies to providers of routers and connecting lines. Moreover, the Directive 97/66/EC shall apply also to Internet Service

Providers (ISPs) providing hosting services, such as portal services, who may log the requests, the referring pages and post cookies on the hard disk of the user and make profiles. The latter is, however, arguable since the host service providers transmit content information and thus it should rather come under the general data protection Directive. The working document recognises that the applicability of the Directive 97/66/EC to the activities of the host service providers is not always clear. When the provider hosts its own portal site comes under the general data protection directive whilst it comes under the specific when he plays the role of the access service provider.

The providers of Internet services, dependent on the aforementioned distinctions, are subject to the obligations to confidentiality and security laid down in both Directives (art. 4, 5 97/66/EC, art. 6 - 8, 16, 17 95/46/EC). Traffic data provided by providers of routers and connecting lines, ISPs and telecommunication providers shall be protected as content data according to art. 5 of Directive 97/66/EC as this is the case in the proposal for an amendment of 97/66/EC.

Interception of communication is unacceptable unless it fulfils three fundamental criteria in accordance with art. 8 (2) EHRC, and the European Court of Human Rights interpretation of this provision: a legal basis, the need for such a measure in a democratic society, and conformity with one of the legitimate aims listed in the Convention.

The Working party strongly recommends the use and offer of encryption tools by the providers of email services at no additional cost. The providers should also offer secure connection for the transmission of the emails. The need of integrity and authentication should be considered as well.

A means for ensuring encryption is the Secure Socket Layer (SSL) which is implemented in the most popular browsers and establishes a secure channel between the client and server computers. This is achieved by means of encryption and digital certificates. SSL enables the authentication of the server to whom the information shall be sent and the integrity of the data. It does not ensure the authentication of the client. These difficulties shall be overcome by the protocol SET (Secure Electronic Transactions) that provides for confidential transmissions using encryption, authentication of the parties, integrity and non-revocation (through digital signatures). The Working Party seems to support the use of the SET protocol instead of SSL, especially when sensitive information, such as the credit cards data, will be transmitted. Moreover, if a higher level of security is needed, the digital certificates should be stored on smart cards.

All the above EV Directives and International Agreements will be fully adopted within GOOD ROUTE. The conformance to them will be safeguarded by the GOOD ROUTE Ethics Committee.

OECD privacy principles

Collection Limitation Principle

"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject".

The limits of the data collection – distinction between necessary and unnecessary data, that will not be stored . will be described within this chapter.

Data Quality Principle

"Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date".

Purpose Specification Principle

"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose".

The purposes will be clearly explained to the participant; never later than during the informed consent process.

Use Limitation Principle

"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance [Purpose Specification Principle] of the OECD Privacy Guidelines except:

- a) with the consent of the data subject; or
- b) by the authority of law".

Security Safeguards Principle

"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data".

Openness Principle

"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the Data Controller".

A task force related to privacy has been established. It will monitor current developments in this field. The nature of the personal data will constantly be scanned, also relating to the planned use. A list of data controllers will be posted.

Individual Participation Principle

"An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

Upon request one of the publicly posted data controllers will deliver the information recorded, if such information exists.

Accountability Principle

"A Data Controller should be accountable for complying with measures which give effect to the principles stated above".

The data controllers will be accountable according to national law of the member states.

Information about your Organisation and your Web Site

Providing visitors to your Web site with information about your organisation, and in particular about the legal entity which controls the processing of personal data, is consistent with the Openness Principle in the OECD Privacy Guidelines. Therefore the information that you provide in this section will be disclosed in your privacy statement so that visitors to your Web sites will know who you are.

Name of the Data Controller

An indication of the name of the data controller is required by the OECD Privacy Guidelines. According to the OECD Privacy Guidelines, "the Data Controller means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf". Therefore the "data controller" may be a legal or natural person, for example, a public authority, an organisation, a department within an organisation, a board of directors, or an individual.

OECD - definitions

Specific Data

According to the OECD Data Quality Principle, personal data should be relevant to the purposes for which they are to be used. In many countries, the personal data listed below are regarded as sensitive and their use restricted. If you collect and use personal data which fall into this category, you should consult the Privacy Resource (for example, the following instruments: Convention 108 of the Council of Europe, European Directive 95/46/EC and the UN Guidelines for the Regulation of Computerised Personal Data Files): Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Health/Medical data, Sex life, Police/Justice data such as civil/criminal actions brought by or against the visitor.

Consent

Seeking consent from visitors for disclosure of their personal data for new purposes accords with both the Purpose Specification Principle and the Use Limitation Principle. The Purpose Specification Principle provides that the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. The Use Limitation Principle develops this further by stating that personal data should not be disclosed, made available or otherwise used for purposes other than those specified. However, if you wish to use or disclose your visitors' personal data for an incompatible and unspecified purpose, you may do so provided that you have obtained consent of your visitors' before proceeding with the new use or disclosure.

Confidentiality/Security

Establishing a security policy that protects personal data under your control is consistent with the Security Safeguards Principle of the OECD Privacy Guidelines.

The **Security Safeguards Principle** implies that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. The 2002 OECD Security Guidelines also recommend that "security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency" under the Democracy Principle.

Security safeguards are intended to reinforce limitations on data use and disclosure. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasised that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality.

Secure Transmission Method

For example if you use an industry standard encryption technology for transferring and receiving personal data on your Web site(s).

Unauthorised Access

For example, steps should be taken to ensure that only authorised staff has access to the data.

Improper Use or Disclosure

For example, steps should be taken to ensure that the data are only used or disclosed for those purposes which were indicated to the visitor at or before the time of collection. Steps may also be taken to confirm the identity of individuals before providing a copy of their personal data to avoid the improper disclosure of one individual's personal data to another individual.

Unauthorised Modification or Alteration

"Modified" should be construed to cover unauthorised input of data. Steps should be taken to ensure that the data are only altered/modified by authorised staff, and are not altered in such a way as would make the data inaccurate.

Unlawful Destruction or Accidental Loss

"Loss" of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage medium. Steps should be taken to ensure that adequate security procedures are in place to prevent any person from either unlawfully (i.e. not in accordance with the data controller's instructions) or accidentally destroying and losing the data.

Data Processors

Data Processors are third parties that process data on behalf of a Data Controller only for the completion of stated purposes, and who do nothing further with the data

Proof of Identity

If you require proof of identity before providing an individual with information about the personal data you hold, or providing a copy of the personal data held, you may wish to indicate the proof you require in your privacy policy statement - for example, a password, confirmation of date of birth, etc.

Directive 97/66/EC on Data Protection in the Telecommunications Sector

This Directive applies to data processed in connection with the provision of telecommunication services in public telecommunications networks, in particular via ISDN and public digital mobile networks, and is aiming to protect the privacy right of natural persons, as well as the legitimate interests of legal entities. Non-publicly available telecommunications services fall within the scope of the general data protection Directive 95/46/EC (Recital 11 Directive 97/66/EC).

The Directive imposes to the telecommunications network provider and the provider of a publicly available telecommunications services a duty to safeguard the privacy of the users. This means that the service provider - if necessary in conjunction with network provider - shall ensure the security of its services in a similar way as under the Directive 95/46/EC. Moreover, the Member States shall take all relevant legal measures to ensure the confidentiality of communications, i.e. to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications without the consent of the users except when legally authorised, for instance for reasons of public security, prevention, investigation, detection and prosecution of criminal offences.

The Directive stipulates the right to privacy with regard to traffic and billing data, itemised billing, the presentation and restriction of calling and connected line identification and the unsolicited commercial calls. For example, alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, such as the use of calling cards, or the deletion of a certain number of digits from the called numbers mentioned in itemised bills. Traffic and billing data must be erased or made anonymous after a period during which the bill may be lawfully challenged or payment may be pursued.

With regard to calling line identification, the calling and the called user must have the possibility via a simple means, free of charge to prevent the presentation of the calling line identification of incoming calls. In the medical context the right of the calling party to keep his/her anonymity should be stressed. In particular, help-lines for some groups of patients such as HIV patients have an interest in guaranteeing the anonymity of their callers.

In case of unsolicited calls for direct marketing the Member States are free to choose between the opt-in or opt-out alternative to protect the users of the services. The opt-in or opt-out alternative means whether such call is allowed on the imperative of prior consent of the user only or in respect to users who stated that they do not wish to receive such calls. The opt-in alternative is, however, prescribed where automated calling systems without human intervention or facsimile machines are used.

However, short time after the transposition of the Directive in the Member States, this shall be amended in order to keep pace with the speedy technological developments. In July 2000 the Commission submitted a proposal for a revised Directive.

It is true, that the wording of the current Directive caused a series of discussions and/or different interpretations whether the Directive is applicable to all kind of electronic communications. In fact, the Directive uses a terminology based on ISDN technology. Terms such as "calls" allude to traditional and ISDN telephony and make its applicability difficult to Internet services. European Commission's intention is now to ensure the protection of the right to privacy on the Internet.

The term "calls" is replaced by the term "electronic communications" and "electronic communications services". The notion "calls" will be further used only where the legislator envisages the telephone calls. The term "electronic communications services" is defined, in art. 2 b) of the proposed Directive establishing a common framework for electronic communication services and networks. Accordingly, electronic communications services include transmission and routing of signals on electronic communications networks. Thus, within the scope of the revised Directive would fall the Internet Service Providers, such as the Access Service Providers. - Content service providers do not fall within this scope -. By the replacement of the term "call" through the term "electronic communications" packet switched transmissions are covered without any doubt.

With regard to traffic data, the revised Directive extends the confidentiality of communications to traffic data. This has been regarded as a very positive measure, since on Internet it is difficult to separate in technical terms between content and traffic data. Login data, amount of data transferred, time and ending of session should be included within the scope of current Art. 6 Directive 97/66/EC. The revised Directive would in addition cover traffic data, such as protocol headers (TCP-header, IP-header etc.) which are read in every router a packet passes through, header information (which might include content information). Traffic data shall be erased upon the termination of the call or in the revised Directive upon termination of the transmission (Data protection working party, 2000).

The revised Directive introduces the possibility of further processing for the provision of value-added services if the subscriber has given his/her consent. Value-added services, might be offered if location data are processed. Location data which allows the exact positioning of a user shall only be used with the consent of the subscriber. The subscribers shall also be provided with a simple means to temporarily deny processing of their location data in the same way as such means exist for calling line identification. The only exception to the principle of prior consent would be the use of location data by emergency services and for purposes of public and national security and criminal investigations.

Finally, unsolicited commercial communication by the use of e-mail would be permitted only upon prior consent of the subscriber (opt-in alternative).

In on-line networks, hence, both Directives should be taken into account. The general Directive 95/46/EC on the protection of personal data is the relevant text to define the obligations of the person who initiates the processing of content data. The Directive 97/66/EC, on the other hand, establishes the obligations of the providers of services pertaining to the transmission of messages or the provision of access services. For instance, in case of transmission of emails the controller should be the person from whom the message originates

and not the person providing the transmission service. The latter will be responsible to safeguard the security of the network and he will be deemed the controller only in respect to the additional personal data processed for the rendering of the service.