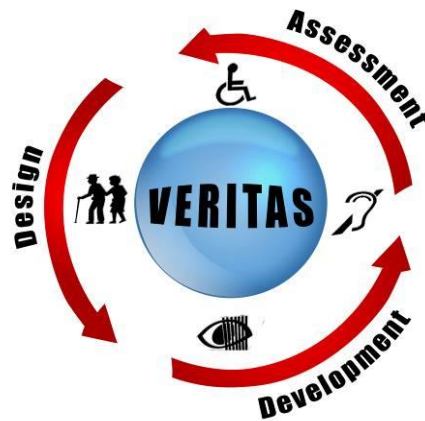


# Accessible and Assistive ICT



## VERITAS

Virtual and Augmented Environments and Realistic User Interactions To achieve Embedded Accessibility DesignS

247765

### VERITAS Ethics Manual

Deliverable No.		<b>D4.1.4</b>	
SubProject No.	<b>SP4</b>	SubProject Title	<b>Horizontal activities</b>
Workpackage No.	<b>W4.1</b>	Workpackage Title	<b>Project management</b>
Activity No.	<b>A4.1.5</b>	Activity Title	<b>Ethical Issues</b>
Authors		<b>Marcel Delahaye, Vitaliy Kolodyazhniy, Marc Graf (COAT-Basel)</b>	
Status		F (Final)	
Dissemination level		<b>Pu (Public)</b>	
File Name:		<b>VERITAS_D414_Ethics_Manual.doc</b>	
Project start date and duration		<b>01 January 2010, 48 Months</b>	



## Version History table

<b>Date</b>	<b>Version</b>	<b>Comments</b>
20.04.2010	1	First version ready, with all the content, questionnaires and the members of the Ethics Advisory Board. Sent for quality review.
27.05.2010	2	Final draft version, after the improvements according to the Quality Improvement Report suggestions.
10.05.2010	3	Final draft version, send for peer review.
11.06.2010	4	Final version, send to the Commission.
September 2010	5	Update the final version according the commends of the review.

# Table of Contents

<b>VERSION HISTORY TABLE .....</b>	<b>3</b>
<b>TABLE OF CONTENTS.....</b>	<b>I</b>
<b>LIST OF TABLES .....</b>	<b>III</b>
<b>LIST OF FIGURES.....</b>	<b>III</b>
<b>ABBREVIATIONS LIST .....</b>	<b>IV</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>2</b>
<b>1 INTRODUCTION .....</b>	<b>5</b>
1.1 PROJECT BACKGROUND .....	5
1.2 THE TEMPLATES ON ETHICAL AND LEGAL ISSUES .....	8
<b>2 INFORMED CONSENT .....</b>	<b>10</b>
1.3 BASIC ELEMENTS OF INFORMED CONSENT.....	10
1.4 GUIDELINES FOR COMPILING THE INFORMED CONSENT FORM.....	11
1.5 INFORMED CONSENT CONCERNING THE USE OF PRIVATE INFORMATION .....	12
1.6 PARTICIPANT GROUPS AND THEIR CONSENT .....	13
1.7 INFORMED CONSENT AND PEOPLE WITH COGNITIVE IMPAIRMENTS/ LEARNING DIFFICULTIES .....	14
1.8 INFORMED CONSENT AND THOSE UNABLE TO READ THE FORM .....	14
1.1.1 <i>Informed Consent and the illiterate</i> .....	14
1.9 THE LEGAL POSITIONS.....	14
1.10 DOCUMENTATION OF INFORMED CONSENT.....	15
1.1.2 <i>Healthy and able bodied participants</i> .....	15
1.1.1.1 Research participant's identity.....	15
1.1.1.2 Participant Consent Form.....	15
1.1.1.3 Investigators' confirming statement .....	15
1.1.3 <i>MI people with motor problems</i> .....	15
1.1.4 <i>Deaf and people with hearing problems</i> .....	16
1.1.5 <i>Informed consent and those unable to read the form</i> .....	16
1.1.6 <i>Illiterate participants</i> .....	16
1.1.7 <i>People with cognitive impairments/learning difficulties</i> .....	16
<b>3 DATA MANAGEMENT .....</b>	<b>17</b>
1.11 ROLE AND DESCRIPTION OF CRITICAL ACTIONS AND GOALS WITHIN VERITAS REGARDING PRIVACY AND SAFETY OF PARTICIPANTS .....	17
1.12 VERITAS PRIVACY POLICY ON COLLECTED DATA.....	20
1.1.8 <i>VERITAS system</i> .....	20
1.1.9 <i>During Preliminary Data Gathering (WP 2), Pilots (WP 3) and Training (WP 4)</i> .....	20
<b>4 PROPOSED SECURITY ISSUES IN VERITAS .....</b>	<b>21</b>
1.13 INTRODUCTION - THE NEED FOR SECURITY .....	21
1.14 FUNDAMENTALS OF VERITAS SECURITY AND DATA PRIVACY .....	22
1.1.10 <i>Main concepts</i> .....	22
1.1.1.4 Authentication .....	22
1.1.1.5 Authorization .....	22
1.1.1.6 Confidentiality.....	22
1.1.1.7 Anonymity.....	23
1.1.1.8 Non-repudiation.....	23
1.1.1.9 Accountability .....	24
1.1.1.10 Integrity.....	24
1.1.1.11 Availability.....	24
1.1.11 <i>Security fundaments</i> .....	25
1.1.1.12 Cryptography.....	25
1.1.1.13 Security design .....	25

1.1.1.14	PKI Infrastructure .....	27
1.1.1.15	Intrusion detection systems .....	27
1.1.1.16	Intrusion prevention systems .....	28
1.1.1.17	Central logs .....	28
1.1.1.18	Failure monitoring systems (FMS) .....	28
<b>5</b>	<b>APPLIED PRIVACY ISSUES .....</b>	<b>30</b>
1.15	GENERAL PRINCIPLES .....	30
1.16	ANONYMISATION AND CODING .....	31
1.17	INTERNATIONAL AND EUROPEAN INSTRUMENTS IN THE FIELD OF DATA PROTECTION .....	32
1.1.12	<i>Data Protection Directive 95/46/EC</i> .....	34
1.1.13	<i>Directive 97/66/EC on Data Protection in the Telecommunications Sector</i> .....	37
1.1.14	<i>Art. 29 - Data Protection Working Party: Working Document on Privacy on the Internet</i> 39	
<b>6</b>	<b>RISK ASSESSMENT, DELEGATION OF CONTROL, DECEPTION AND DEBRIEFING .....</b>	<b>41</b>
1.18	AMI CONTROL LEVEL VS PERSON'S CONTROL LEVEL .....	42
1.19	DECEPTION .....	42
1.20	DEBRIEFING .....	43
<b>7</b>	<b>ORGANIZATION AND INSURANCE ISSUES .....</b>	<b>44</b>
1.21	ETHICS CONTROL COMMITTEE .....	44
1.22	ACCESSIBILITY OF FACILITIES AND SERVICES .....	44
1.23	REIMBURSEMENT SCHEMES .....	44
1.1.15	<i>Incentives for research respondents</i> .....	44
1.1.16	<i>Legal basis for reimbursements as incentives</i> .....	45
1.1.17	<i>The amount to pay</i> .....	45
1.1.18	<i>Type of payment</i> .....	46
<b>8</b>	<b>ETHICAL ISSUES ACROSS THE PROJECT LIFE-CYCLE .....</b>	<b>47</b>
1.24	METHODOLOGY .....	47
1.25	VERITAS ETHICS ADVISORY BOARD .....	48
1.26	EXPLANATION .....	50
1.27	CLARIFICATION OF THE ROLE OF THE ETHICS ADVISORY BOARD (EAB) .....	50
1.28	EAB TERMS OF REFERENCE .....	51
1.29	ETHICS SITE RESPONSIBLE .....	52
1.30	VERITAS ETHICS CONTROL AT THE PILOT AND TRAINING SITES .....	54
1.1.19	<i>Workshop for the Pilot sites</i> .....	55
<b>9</b>	<b>GENERAL LEGAL FRAMEWORK FOR THE RESPECTIVE EUROPEAN COUNTRIES: RELEVANT LOCAL ETHICS RESEARCH COMMITTEES .....</b>	<b>56</b>
1.31	LEGITIMACY ISSUES OF VERITAS .....	56
1.32	LEGAL ISSUES .....	57
1.33	MEDICAL DATA IS PERSONAL DATA .....	58
1.34	RELEVANT PROVISIONS OF THE DATA PROTECTION DIRECTIVE .....	58
1.35	PRIVACY GUIDANCE IN TECHNOLOGY DESIGN .....	60
1.36	TRANSPARENCY .....	60
1.37	CONSENT .....	60
1.38	PROPORTIONALITY, LIMITATION .....	61
1.39	SECURITY AND IDENTITY THEFT .....	61
1.40	SUMMARY (VERITAS ETHICS RULES) .....	62
<b>10</b>	<b>LREC: LOCAL RESEARCH ETHICS COMMITTEES .....</b>	<b>64</b>
1.41	UK .....	64
1.1.20	<i>Summary of UK RECs</i> .....	66
1.42	FRANCE .....	68
1.1.21	<i>Summary of French RECs</i> .....	69

1.43	GERMANY .....	74
1.1.22	Summary of German RECs .....	76
1.44	BELGIUM .....	78
1.1.23	Summary of Belgian RECs .....	78
1.45	GREECE .....	79
1.1.24	Summary of Greek RECs.....	81
1.46	ITALY .....	82
1.1.25	Summary of Italian RECs.....	83
1.47	BULGARIA .....	86
1.1.26	Summary of Bulgarian RECs.....	88
<b>11</b>	<b>DETECTION AND MANAGEMENT OF ETHICAL CONCERNS OF PEOPLE AFFECTED BY DISABILITIES DURING THE WHOLE PROJECT PHASE .....</b>	<b>90</b>
<b>12</b>	<b>CONCLUSIONS .....</b>	<b>91</b>
<b>13</b>	<b>REFERENCES.....</b>	<b>92</b>
	<b>ANNEX 1 QUESTIONNAIRE ON ETHICAL AND LEGAL ISSUES .....</b>	<b>94</b>
	<b>ANNEX 2 VERITAS INFORMED CONSENT FORM TEMPLATE .....</b>	<b>105</b>
	<b>ANNEX 3 ORGANISATIONAL AND INSURANCE ISSUES.....</b>	<b>111</b>
	<b>ANNEX 4 INSTRUCTIONS FOR COMMUNICATION WITH DEAF PEOPLE .....</b>	<b>116</b>
	<b>ANNEX 5 INTERVIEWS WITH DISABLED PEOPLE - GUIDELINES .....</b>	<b>117</b>
	<b>ANNEX 6 COMMUNICATING WITH BLIND AND PARTIALLY SIGHTED PEOPLE .....</b>	<b>121</b>
	<b>ANNEX 7 OFFICIAL DEFINITIONS/PRINCIPLES APPLIED.....</b>	<b>127</b>
	<b>ANNEX 8 QUESTIONNAIRE ON PERSONAL INFORMATION .....</b>	<b>132</b>
	<b>ANNEX 9: ETHICAL PILOT APPLICATION FORM.....</b>	<b>136</b>
	<b>ANNEX 9: ETHICAL PILOT APPLICATION FORM.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>

## List of tables

Table 1	Pilots for designers and developers .....	3
Table 2	Application domains and end-user categories .....	3
Table 3:	Physical attributes and the possible Medical Diagnose .....	19
Table 4	Partners responsible for ethics safeguard. ....	53
Table 5	Summary of UK RECs. ....	67
Table 6	Summary of France RECs. ....	73
Table 7	Summary of German RECs.....	77
Table 8	Summary of Belgian RECs.....	79
Table 9	Summary of Greek RECs.....	82
Table 10	Summary of Italian RECs. ....	86
Table 11	Summary of Bulgarian RECs. ....	89

## List of figures

Figure 1:	Ethical Management procedure. ....	49
-----------	------------------------------------	----

## Abbreviations List

<b>Abbreviation</b>	<b>Definition</b>
DoS	Denial of Services
EFGCP	European Forum for Good Clinical Practice
EHRC	European Human Rights Court
EIS	European Information Society
IDS	Intrusion Detection System
ITT	Invitation to Tender
ISP	Internet Service Provider
LED	Light Emitting Diode
LREC	Local Research Ethics Committee
NIDS	Network Intrusion Detection System
PKI	Public Key Infrastructure
PoP	Proof of Possession
SET	Secure Electronic Transaction
TPD	Trusted Personal Device
UCD	User Centered Design
UMTS	Universal Mobile Telecommunication System
WoZ	Wizard of Oz



## EXECUTIVE SUMMARY

**The current Ethics Manual** defines the ethics code of conduct of research within VERITAS. Within this document, the key ethical and legal issues will be identified and a relevant project policy towards examining these issues will be developed.

Two basic ethical issues are related to the project conduct.

1. The performance and set up of the pilots (WP3), and the training of different end user groups (WP4), as well as the preliminary user feedback in WP2, the comfort and safety of all participants has to be guaranteed, as well as the security and legal issues of their personal data (e.g. related to their special needs and preferences). Specific guidelines from the EFGCP (the European Forum for Good Clinical Practice) are given in this Manual to the ethical and legal issues for vulnerable users (elderly and disabled people). For this, a specific section related to 'VERITAS Ethics control at the pilot and training sites' is prepared (Chapter 8). In the duration of the project the pilot plans (D3.6.1; D3.7.1; D3.8.1) will be checked by the Ethics Advisory Board, which has been set up by COAT. These members will report their comments and these will be included, together with partners' feedback, and the emanating Deliverable changes will be added – if necessary – in the project pilot plans Deliverable (final version).
2. The project developments as a whole, in a way that guarantees that future products and services are being ethically designed for all people including those with disabilities and avoids the creation of barriers, as well as the protection of their personal data (health status, capacities, abilities, location, routing, etc.).

**The current Ethics Manual** can be regarded as an **ADDENDUM** which enhances the Ethics Manual due to the review comments (30.06.2010), which were:

1. Specification of the role and tasks of the Ethics Advisory Board (especially the interaction with the project partners); see chapter 8
2. More specific definition of a legal ethical framework at European Level and description of the ethical framework of the specific countries where data collection takes place; see chapter 9 and 10
3. Detection and Management of Ethical Concerns of people affected by disabilities during the whole project phase/ Contingency plan for addressing potentially occurring ethical risks; see chapter 11

Within the scope of VERITAS, two different pilot sets are involved:

First, the **pilots for developers and designers** will be organized at 4 pilot sites countries (Germany, Greece, Italy, UK) (see WP3.7): at the end of the 2nd year and during the 3rd year and will involve 140 developers/designers. The piloting will consist of iterative evaluation and testing cycles. Relevant Deliverables for the methodology are D1.1.2 "UCD design guidelines for applications development", as well as D3.6.1 "Pilot Planning and Evaluation Framework" and

the both Deliverables in WP 3.7. The overall site piloting organisation is clarified in the table below:

	<b>Application field</b>	<b>Test site in countries</b>	<b>Total number of participants (developers and designers)</b>
1.	Automotive	DE, UK, GR	30
2.	Smart Living Spaces	DE, UK, GR	50
3.	Office workplace	DE, UK, GR	30
4.	Infotainment and Games	UK, GR	20
5.	Personal Healthcare and Well-Being	IT	10

**Table 1 Pilots for designers and developers**

Second, the **pilots for the end-user, also called beneficiaries** (people with disabilities and older people) will take place at 5 pilot sites (Belgium, Bulgaria, Italy, Greece and the UK). Within the scope of VERITAS, 380 participants will be tested. Before each pilot of VERITAS' 5 application fields will be preceded by a dedicated demo event during which the local pilot users will be able to get themselves accustomed with VERITAS tools. The end-user groups are: Blind and low-vision users, Motor impairment users, Cognitive impairment users, Hearing impairment users and speech impairment users. The relevant WP for end-user and impaired participants is WP3.8.

For each application domain, end user groups will be defined and used to test the designs developed in WP3.1, WP3.2, WP3.3 and WP3.4 based on the evaluation framework developed in WP3.6 (Iterative Pilots and Pilot Planning). The overall site piloting organisation is clarified in the below table. Respective countries are not specified yet:

	<b>Application field</b>	<b>Blind and low vision users</b>	<b>Motor impairment users</b>	<b>Cognitive impairment users</b>	<b>Hearing impairment users</b>	<b>Speech impairment users</b>
1.	Automotive		X	X	X	
2.	Smart Living Spaces	X	X		X	X
3.	Office workplace	X	X	X	X	X
4.	Infotainment and Games	X	X	X	X	X
5.	Personal Healthcare and Wellbeing	X	X	X	X	X

**Table 2 Application domains and end-user categories**

In general it is the code of conduct for the project, that all project partners' Deliverables and pilots conduct will be scanned on behalf of the information listed in this manual. Relevant international and European conventions (e.g. Helsinki Declaration) are fully integrated in this manual. In the course of the

project, also all national legislations will be fully integrated (e. g. Ethical approval for the pilots). In utilising the 'Template on ethical and legal issues' (ANNEX I) for those partners conducting training, pilots, or any kind of data collection, specific national standards and local conventions of ethics committees are being scanned and integrated. All in all, this manual is conceptualised to offer guidelines for all research performed within the auspices of VERITAS.

After an introduction, in which the VERITAS project is described (Chapter 1), detailed information about the informed consent, such as basic elements and guidelines for compiling the Informed Consent form, is provided (Chapter 2). This is based upon the informed consent template, which clearly demonstrates the privacy protection policies of the project. Also the issue of conducting experiments with people, who have learning or cognition (i.e. memory, concentration, or divided attention) difficulties, such as elderly (but not mentally or cognitive disabled) is provided. Finally, detailed guidelines on how to document the informed consent process regarding the different user groups are listed (people with special needs). Chapter 3 defines the Data Management Strategy of the project, including which data will be stored by VERITAS system and which data will be kept by the pilot trials participants, as well as how they will be managed. Privacy issues are also dealt within Chapter 3. Chapter 4 is about the proposed IT security of VERITAS. Chapter 5 is about the VERITAS Applied Privacy Issues, concerning the issue on how confidentiality of personal data can be maintained and guaranteed, based upon different methods of anonymisation that are listed. Chapter 6 is about risk assessment, delegation of control, deception and debriefing. Different categories of risks are listed, concluding that it is very important to take into account the prospective participants' view of the importance of risk. The end point of this process is the informed consent, given by the prospective participant. In Chapter 7 organization and insurance issues are described. The VERITAS Ethical issues across the project life-cycle are described in Chapter 8, including a methodology part (including the Ethical Checklist), in which it is described how information on ethical issues is being collected. In the same chapter, the VERITAS Ethics Advisory Board is listed, as well as the way that the VERITAS Ethical Policy is applied to its pilot sites. Last but not least, conclusions follow in Chapter 9.

In the Annexes, some instructions on how to communicate with deaf and other disabled people and relevant documents can be found, as well as all relevant questionnaires and templates.

# 1 Introduction

VERITAS is a large and complex project, with ethical issues related to security, privacy and accessibility. In order to achieve a successful outcome, it is essential that basic requirements of the users and the ethical, legal and technological framework are respected. The project will comply with these issues by implementing relevant solutions.

These moral and ethical issues can centre on personal freedom, autonomy, privacy, or responsibility. Special background for this Manual was the book: "Safeguards in a World of Ambient Intelligence by David Wright et al (Springer 2008)1).<sup>1</sup> *Wright, D. Gutwirth, S. Friedewald, M. Vildjiounaite, E., Punie, Y.; Safeguards in a World of Ambient Intelligence , The International Library of Ethics, Law and Technology 1, Springer, 2008 .*

Within this document, ethical and legal issues with regard to VERITAS are discussed in such a way, that potential ethical and legal aspects are identified and briefly analyzed.

## 1.1 Project background

The core concept of VERITAS is to conduct research and development of an open framework for providing built-in accessibility support at all the stages of realisation of mainstream ICT and non- ICT technologies. The project aims at delivering to product/software developers 'generic' instructions - embedded in an empowering virtual reality platform, for exploring new concepts, designing new interfaces and testing interactive prototypes that will inherit universal accessibility features, including compatibility with established assistive technologies.

The main VERITAS innovation lies in the fact that, even if there have been some limited and isolated attempts to support accessibility testing of novel products and applications, there is a clear lack of a holistic framework that supports comprehensively virtual user modelling, simulation and testing at all development stages and realistic/immersive experience of the simulation.

VERITAS aims to develop, validate and assess tools for built-in accessibility support at all stages of ICT and non-ICT product development, including specification, design, development and testing. The goal is to introduce simulation-based and virtual reality testing at all stages of assistive technologies product design and development into the automotive, smart living spaces, (buildings & construction, domotics), workplace, infotainment and health applications areas. The goal is to ensure that future products and services are being systematically designed for all people including those with disabilities and functional limitations as well as older people. Furthermore, VERITAS plans to promote its results to the appropriate standards organisations for consideration and potential adoption and also to make them available through an open framework.

In order to give a brief overview about VERITAS, the main project objectives are described below:

- **To translate** the accumulated **knowledge on ICT accessibility** to parameters of the **virtual user models** (including task models) and simulation models for a variety of applications,
- **To test** the validity and applicability of these virtual user models in real accessibility testing scenarios using an **innovative multisensorial platform**,
- **To create a set of simulation models** building on the experience already gathered via testing accessibility in various applications domains
- **To integrate** all the above into VERITAS knowledge, which will serve as a reference to the existing ICT accessibility know how
- **To provide support to the developers and designers** at all the stages of product development
- **To export** the virtual user and the simulation **models to existing developer/design** platforms that are already used for the design/development of mainstream ICT and non-ICT products
- **To investigate and develop an open library** of various categories of **virtual user models**, including VR models, covering a wide range of population groups and especially focusing on groups in risk of exclusion, e.g. older people, people with disability (vision, hearing, speech, motor), people with co-existent condition, etc.
- **To develop an Open Simulation Platform (OSP)** for virtual reality simulation and testing of new products at all stages of iterative product planning and development, i.e. specification, design, development, validation and testing
- **To develop an extensive list of virtual reality tools** for supporting accessibility testing at all stages of development of existing applications, of partners of the VERITAS consortium, in the following domains: a) automotive, b) smart living spaces, c) workplace design, d) infotainment and e) personal healthcare and wellbeing
- **To research and develop methodologies for introducing the VERITAS simulation** and testing framework, including the virtual user and the simulation models, **to a wide variety of ICT and non-ICT applications**
- **To research and develop a framework for immersive virtual user simulation** and testing, i.e. putting the developer in the position of the user through virtual/augmented reality simulation
- **To define measures and metrics for evaluating software accessibility** for every application scenario during design and development through VR simulation (graphs, statistics, distance metrics in general)
- **To research and develop innovative concepts for ambient**, multi-device, universally accessible and usable multimodal interfaces through VR simulation

**Targeted domains:** VERITAS aims at introducing embedded accessibility: developing groundwork, creating infrastructure and establishing standards in the following important domains:

- Design and developer tools
- ICT and non-ICT solutions with special emphasis in the following domains:
  - o Automotive
  - o Smart Living Spaces

- o Workplace
- o Infotainment
- o Personal HealthCare and Wellbeing

**The VERITAS Users and Stakeholders' Groups:** VERITAS mainly addresses 2 categories of end users:

1. Designers and developers of ICT infrastructure, applications and services – referred to hereinafter as “developers”.

2. People with disabilities (including the older people) –referred to hereinafter as “end users”– who experience one or more of the following mild to severe impairments:

- Blind and low-vision impairments
- Motor impairments
- Cognitive impairments
- Hearing impairments
- Speech impairments

The specific impairment sub-groups that will constitute target groups of the VERITAS project are provided below. In the Annexes, some instructions on how to communicate with deaf and other disabled people and relevant documents can be found, as well as all relevant questionnaires and templates.

### **People with disabilities**

- Blind and low-vision impairments
  - Light or moderate limitations (visual acuity, slow accommodation, etc)
  - Reduced field of vision
  - Limited night and color vision
  - Severe limitations, blindness
- Motor impairments
  - Lower limb impairments (Limitations in motion or strength or coordination or anthropometric limitations of lower limbs)
  - Wheelchair users (Limitations in motion or strength or coordination or anthropometric limitations of lower limbs resulting in use of wheelchair)
  - Upper limb impairment (Limitations in motion or strength or coordination or anthropometric limitations of upper limbs and touch limitations)
  - Upper body impairment (Limitations in motion or strength or coordination of upper body (head and trunk))
- Cognitive impairments
  - Visual and auditory word recognition impairment
  - Limitations in information processing
- Hearing impairments
  - Light or moderate limitation
  - Severe limitation or total deafness
- Speech impairments
  - No speech or very limited speech

- No speaking or very limited speaking local language
- Low volume of speech
  
- Older people (= OASIS user group categorization will be applied)
  - Independent
    - Living at home
  - Dependent
    - Living at home
    - Not living at home

Each of these user groups have very specific disability related handicaps in the automotive, smart living spaces, workplace, infotainment and personal healthcare environment, thus will also provide much needed input to the user requirements and ultimately will also participate in the WP 3.8: “Pilots for the end-users”.

Beside these user groups. other stakeholders are involved as well such as:

- ICT providers (industrial players and SMEs)
- National, local and regional authorities
- Assistive Technology providers (both hardware and software)
- Service providers, specifically for people with disabilities and older people
- Family members • Disability groups, forums and Associations
- Public / private Social security service providers and insurance companies
- Mobile service providers
- Health care and emergency support service providers
- Policy makers / standardisation bodies

As you can see from the list above an enormous number of people with different interest might have access to very sensitive (even health) data. Therefore, the dignity, rights, safety and wellbeing of test participants must be a primary consideration of any research study. Within this VERITAS Ethics Manual, entitled (at hand), background information concerning the recognition of key ethical and legal issues is provided. A relevant project policy is being developed (ethics code of conduct). It is specified which data are essential for the project and which will be excluded from retention (especially any information which could be linked with the identity of a participant, as well as any religious or philosophical beliefs, political opinions or sexual phantasy or experience). Based on the information provided in this handbook, all project partners' deliverables will be scanned by the Ethical Manager (COAT). All relevant national and international European conventions (i.e. Helsinki Declaration) are fully integrated. With the aid of the 'Template on ethical and legal issues', national standards and the norms of Local Ethics Research Committees will be gathered. Within the Ethics manual, the ethical frame for the conduct of the pilots and various trainings will be also justified on scientific and legal basis in depth.

## 1.2 The templates on ethical and legal issues

The data collection is divided in following parts:

- questionnaire on ethical and legal issues (ANNEX 1),

- the documents for the informed consent (ANNEX 2),
- questionnaire about organizational and insurance issues (ANNEX 3),
- questionnaire on personal information (ANNEX 8)

The questionnaire on ethical and legal issues has to be filled in by the investigator who conducts pilots, trainings or any kind of data collection. It is also a sort of preliminary checklist, in which the researcher is reminded to take into account all the relevant ethical aspects before conducting any experiment. This questionnaire on ethical and legal issues is divided into different subsections (informed consent, ethical control instruments, privacy, safety, risk assessment). All pilot partners need to fill in and send the questionnaires to COAT. In the current document the results will be reviewed by the Ethics Advisory Board and summarized in the (revised) Ethics handbook.

Informed consent documents are annexed to the questionnaire. With the aid of those, the informed consent will be also documented; see also section 2.8 *Documentation of informed consent*.

Concerning **illiterate participants**, oral consent in the presence of at least one witness may be given (according to Article 3 d) of Directive 2001 / 20 / EC (2001)). This witness has to sign the informed consent document no 3.6 (Listed under – VERITAS-Informed consent template, Paragraph 3). With question 9, we check if the consent given by a witness for an illiterate participant is in accordance with the national legislation. Information regarding this issue follows within the Subchapter 2.6.1 *Informed consent and the illiterate*.

The purpose of the section ‘organizational and insurance issues’ (Annex 3) is to highlight the organizational issues, that the partners have to follow, like accessibility of facilities and services and different reimbursement schemes (legal basis for reimbursement, amount and type of payment, insurance provision) for end-users involved as interviewees, participants or training subjects. In this context a questionnaire section for organizational and insurance issues is annexed to this document.

## 2 Informed consent

Informed consent is the process by which a **pilot, study and training participant** will be fully informed about the research in which he/she is 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: the information given, the capacity to understand it and the voluntariness of any decision taken.

Respect for persons requires that participants are 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).

### 2.1 Basic elements of informed consent

All investigators within VERITAS will seek the informed consent of the user, only under circumstances that provide the prospective participant sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence.

The information that is given to the participant or the representative will be in a language understandable to the participant.

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:

- a. Appropriate insurance or indemnity to cover the participant in trial should be provided.
- b. A table of certified sensors and/or software as well as the prototypes not yet certified that shall be used by the patient underlying the potential risks and legal binds that may be in effect 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 which are currently unforeseeable (the case being very unlikely within VERITAS);
2. anticipated circumstances under which the participant's participation may be terminated by the investigator without regard to the participant's consent;
3. the consequences of a participant's decision to withdraw from the research and procedures for orderly termination of participation by the participant;
4. 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
5. the approximate number of participants involved in the study.

## 2.2 Guidelines for compiling the informed consent form

The following comments may help investigators 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 in VERITAS 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 must be described.
- The human participants will be informed of the reasonably foreseeable harms, discomforts, inconveniences and risks that are associated with the research activity. If additional risks are identified during the course of the research, the consent process and documentation will be revised to inform participants as they are re-contacted or newly contacted.
- **The benefits** that participants may reasonably expect to encounter will be described. There may be none other than a sense of helping the public at large. If payment is given to defray the incurred expense for participation, it must not be coercive in amount or method of distribution.
- The participants are told the extent to which their **personally identifiable private information** will be held in confidence. See also the chapters about data management, security and privacy (chapters 3 & 4).
- If **research-related injury** (i.e. physical, psychological, social, financial, or otherwise) is possible, that is more than minimal risk, an explanation will be given of whatever voluntary compensation and treatment will be provided (not expected to be the case within VERITAS).
- **The legal rights of participants will not be waived in any way.** The participants should not be given the impression that they have agreed to and are without recourse to seek satisfaction beyond the institution's voluntarily chosen limits.
- **Details of contact persons** who are able to answer questions of participants about research, rights as a research participant, and research-related injuries will be provided.

A single person is not likely to be appropriate to answer questions in all areas. This is because of potential conflicts of interest or the appearance of such. Questions about the research are most often best answered by the investigator(s). However, questions about the rights of research participants or research-related injuries (where applicable) may best be answered by the on-site doctor for instance (especially in the health domain). These questions can also be addressed to the investigator, an ombudsman, an ethics committee, or other informed administrative body. The informed consent document will contain contact information with local telephone numbers to answer questions in specified areas.

- 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.

### 2.3 Informed consent concerning the use of private information

Within VERITAS, personal data - according to the definition of the OECD and the Directive 95/46/EC- will be recorded. A concise description of which data

will be stored and which will not, is provided in chapter about data management. The participant will be fully informed about:

- Research purpose (as stated in the chapters *basic elements of informed consent and guidelines for compiling the informed consent*).
- What kind of data will be recorded, stored and why?
- Will the data be transferred?
- Data ownership?
- Is the data connected to other information?
- Will the data possibly commercially exploited?
- Length of storage?
- Where data will be stored, - according to which national legislation?
- Who will access the data?
- Who will supervise the data protection?

## 2.4 Participant groups and their consent

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.

In the context of VERITAS, the following sub-divisions give some indication about the groups of mobility impaired people (elderly, disabled) that may be involved in the project (see also chapter 1):

- blind/partially sighted people;
- deaf and people with hearing problems;
- people unable to walk, i.e., wheelchair users;
- people who have difficulty in walking and bending limbs;
- people who have medical problems affecting balance and stamina;
- people with mild cognitive impairments/learning difficulties (not classified as disabled; mainly elderly);
- people who are illiterate.

Informed Consent is crucial in all aspects of social research and particular attention will be given, when disabled people are involved, that rights are protected and compliance is always freely entered into. 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.

People who are unable or do have difficulties to walk and people who have medical problems affecting balance and stamina, with no further cognitive impairments, are generally able to give a valid consent, that is not different from the one of healthy and able bodied participants. For participants that are deaf or who have hearing problems, the informed consent has to be provided in a modality that they are able to understand, in this case not in auditory mode. There are groups of participants with which standard procedures used for informed consent are not appropriate. Illiterate people have no limitations in cognitively understanding the trial and are able to give verbal consent (e.g. on

audiocassettes to be reviewed), but as they are unable to write, they cannot sign a written informed consent form that is used for documentation. This matter is discussed in chapter 2.6.1 *Informed consent and the illiterate* (SRA, 2003).

For those unable to read the consent form (blind and partially sighted, dyslexic, illiterate) an ordinary documentation of informed consent is also not appropriate. For these people the information will be provided in appropriate alternative media (e. g. large print, audio tape, braille).

## 2.5 Informed consent and people with cognitive impairments/ learning difficulties

Many people with mental impairment or disorder are capable of giving or withholding consent to their inclusion in research and should be free to do so.

The informed consent information (see chapter about informed consent) will be in very simple language and a lot of time will be given to the people with cognitive impairments to reflect his / her decision of giving or withholding consent.

***The VERITAS user groups do not include mentally disabled people (people unable to give a valid consent); only people with limited learning or cognition (i.e. memory or concentration or divided attention) difficulties, i.e. due to normal ageing. Any person not able to give a valid informed consent must be excluded from VERITAS tests.***

## 2.6 Informed consent and those unable to read the form

There is a range of people who are unable to read the consent form; these include those who have a severe visual problem, those with severe dyslexia, those who are illiterate and those whose knowledge of the language may be limited (e.g. a recent immigrant). For these people the information will be provided in appropriate alternative media (e.g. large print, audio tape, Braille, through translator, etc.).

### 2.6.1 Informed Consent and the illiterate

Directive 2001 / 20 / EC of the European parliament and of the council states that in accordance with Article 3:

A clinical trial may be undertaken only if, in particular:

d) if the individual is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation.

## 2.7 The legal positions

The VERITAS research does not include any treatment. The only relevant legal issue is the handling and protection of private data.

## 2.8 Documentation of informed consent

Informed consent shall be documented by the use of a written consent form, approved by the VERITAS Ethics Advisory Board and signed by the participant or the participant's legally authorized representative. 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 in the previous section.

Templates are provided as Annexes of this document, under VERITAS informed consent form template. According to different test participants groups (with different disabilities) different forms have to be filled in. Form 1 on general information has to be filled in every case. The information under header 2 INFORMATION ON THE RESEARCH STUDY has to be provided to the participant in an appropriate modality e.g. auditory for the illiterate; written for the deaf). According to the disability, different forms under chapter 3 have to be filled in. These are described below.

### 2.8.1 Healthy and able bodied participants

In the case of an experiment with a **healthy and able bodied participants**, forms:

See ANNEX II, Part 3

#### 2.8.1.1 Research participant's identity

*Will be filled in by the participant.*

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

#### 2.8.1.2 Participant Consent Form

*Will be filled in by the participant.*

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

#### 2.8.1.3 Investigators' confirming statement

*This part will be filled in by the investigator.*

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

### 2.8.2 MI people with motor problems

This group includes:

- people unable to walk, i.e., wheelchair users;
- people who have difficulty in walking and bending limbs;
- people who have medical problems affecting balance and stamina.

These people are fully able to understand the trial and therefore the same forms as for healthy and able bodied participants can be used (Chapter 2.8.1).

### **2.8.3 Deaf and people with hearing problems**

This group of participants is fully able to understand the trial and therefore the same forms as for healthy and able bodied participants can be used. It has to be considered that the informed consent information cannot be provided auditorily!

### **2.8.4 Informed consent and those unable to read the form**

The form 3.1 ,Research participant's identity' will be filled in by the investigator. The form 3.3 will be provided in appropriate alternative media (e.g. large print, audio tape, Braille, through translators, etc.).

### **2.8.5 Illiterate participants**

Oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation (See section 2.7). The witness (person who is present when the illiterate participant has given oral consent) has to sign consent form 3.4.

This template will be of course translated into the national language of the country where the experiment is to be performed. The template will be adapted each time to the local specificities of each national ethical committee.

### **2.8.6 People with cognitive impairments/learning difficulties**

This group of participants is normally able to understand the informed consent information. In the unlikely case that they are unable to do so, no experiment will be conducted.

## 3 Data management

The aim of this chapter is to clarify, that personal (health) data are highly sensitive. During the developmental phase of the products (as well as the final products itself), highly sensitive private data will be transferred and analysed. It is stated in the DoW, that one of the major parts in VERITAS is (beside the development) the testing of the products in the following domains: a) automotive, b) smart living spaces, c) workplace design, d) infotainment and e) personal healthcare and wellbeing.

In the next paragraphs different examples for sensitive data are mentioned for these five categories.

### 3.1 Role and description of critical actions and goals within VERITAS regarding privacy and safety of participants

This section has the primary goal to underline the concrete Ethical Issues of VERITAS. As already mentioned, VERITAS will touch and deal with sensitive data. Having a look at the objectives, it can be stated that VERITAS is aiming: To create virtual user models for all supported categories of older people and people with disabilities. Virtual user models will be created taking into account the physical, cognitive and behavioural/psychological modelling of the users with disability **based on a) the analysis of real user needs and wants**, b) the incorporation of guidelines, standards and methodologies and c) **training with real users and getting feedback through a multisensorial platform**.

The platform will utilize interaction of real users in the virtual environments, in terms of their physical cognitive, behavioural and physiological response, to tune the virtual models and provide sufficient feedback for the quantitative evaluation and verification of the user models.

In the following, a description is provided on how the VERITAS is touching sensitive data. Therefore a save and transparent data management and security is indispensable.

*a) Automotive: informations about the users` health conditions as well as his/her localisation and driving skills might be transferred between different units of the system and between different partners/stakeholders. The users` limited functionalities as well as their physical and cognitive capabilities are analyzed for ergonomic design.*

*b)/c) Smart living/Working place design: information about the users` health conditions, motivation as well as his/her localisation, Living habits (e.g. eating habits, Internet use, etc.) and their communicative activities might be transferred between different units of the system and between different partners/stakeholders. Sensitive data on working performance, perception of new tasks and mental as well as general health conditions are measured.*

*c) Infotainment: information about the users` health conditions as well as private preferences might be transferred between different units of the system and*

between different partners/stakeholders. The simulation platform is aiming to simulate interaction with the presence of real external participants that will provide a test communication with other players, socializing and all aspects of human behaviour included in the metaverse.

d) *Personal healthcare: information about the users` health conditions might be transferred between different units of the system and between different partners/stakeholders. By focusing on a set of applications (monitoring of physiological and physical parameters through sensors), health coach (education and motivation), drug delivery and therapy management and adherence, the accessibility, the usability and the acceptability of the solutions by the patients will be identified.*

*Personal health data necessarily touch upon the identity and private life of the individual and are thus extremely sensitive. During the pilots in VERITAS **no participant will be exposed to more stress** (within the scope of VERITAS, stressful events could be: to evaluate a tool in VR, which might cause simulator sickness, or might be stressful as the user might not be familiar with VR scenarios and systems) **than necessary**. We clearly declare that nobody will be tested who is in an acute schizophrenic phase or is disillusioned. Only participants with stable mental conditions will be offered to participate. As the mental condition of people can change rapidly (acute symptoms can arise) the participant has to give his/her agreement for the conductance of the pilot participation not more than 24 hours before. The VERITAS consortium is obliged to inform every participant about his/her right to decline whenever he/she wants without giving any reason to do so.*

***Note: In the health domain, no clinical diagnosis will be given without request. A participant will be informed orally that s/he has the right that incidental findings will be sent to his/her GP or psychiatrist if s/he wishes to do so. We do declare that every physiological sample (e.g. EEG sensors, etc.) will be checked in a general screening by a medical doctor, if the participants agrees. During the pilots, important incidental findings can be detected, so we strongly recommend every patient to give his/her agreement that incidental findings can be reported to his/her psychiatrist.***

*Especially for the health domain, no user profile-related information at all is supposed to be stored on the server`s side. All personal information will only be stored on the personal device of the users (and in case of the pilots or training, they will be destroyed).*

***Analysis of real user data captured when performing specific tasks using an innovative parameterised multisensorial platform:***

The main innovation in VERITAS in respect to virtual user modelling is the introduction and use of a multisensorial platform (WP1.2 The Multisensorial Platform) for the training of parameterised user models based on real user measurements in real testing conditions. The multisensorial platform will be fully parameterised and adapted to the VERITAS application areas and will be used to **capture user feedback** while executing a number of tasks that will be

mapped in the VERITAS virtual user models. Special sensors will be used for data capturing ranging from face monitoring cameras for driver monitoring to wearable sensors for body motion analysis, to motion trackers and gait analysis sensors for analysing user kinematic patterns while executing specific activities and tasks and also to environmental sensors for monitoring the interaction of users with the real environment. Different levels have been conceived in the multisensorial platform according to the application contexts. The most critical information will be received in the health domain.

Through the data gathering even in the non health domains, critical information about the health status could be extracted. The table below gives a brief overview about the Physical attribute and the possible Medical Diagnose.

<b>Physical Attribute type &amp; Application domain</b>	<b>Possible Medical Diagnose</b>
Grasping sensors/ Automotive; Smart Living Spaces and Domotics;	Pulse oximeter technology, Congenital heart disease (CHD), Sweat sensors, ridges of the skin are correlated with chromosomal disorders (Down syndrome (1 child in 700), Turner's syndrome (1 woman out of 2000), and Klinefelter's syndrome, nonchromosomal disorders, leukemia, breast cancer, and Rubella syndrome
Vision Smart Living Spaces; Office workplace, Personal HealthCare	Pupillary response; common afflictions like diabetes, arteriosclerosis, and hypertension
ECG/EEG Personal HealthCare	Several Medical conditions & with Emotional responses (nervousness)
Gait Pattern/ texture Smart Living Spaces; Office workplace, Personal HealthCare	Diagnosing Parkinson; overweighted;
Voice pattern/ Facial image Automotive; Smart Living Spaces; Office workplace, Personal HealthCare	Emotional state (anger)/ Vigilance

**Table 3: Physical attributes and the possible Medical Diagnose**

In different phases (initial data gathering, iterative Virtual User Model testing, final evaluation, final demo, pilot organisation) different partners are involved. Therefore all of the mentioned partners below have to appoint an Ethics Responsible (chapter 8.3):

CERTH, RE-LAB, UNEW, CRF, CAF, PIAGGIO, I+, Bauunion, FhG, Domologic, Hypertech, BYTE, MCA, FIMI, UPM,AGE, Smartex, Percro,

## **3.2 VERITAS privacy policy on collected data**

### **3.2.1 VERITAS system**

VERITAS may store some of the following personal data (user profile agent): Age, gender, nationality (language), modality of info (visual or acoustic), functional impairments (according to user groups of VERITAS), and any specific medication taken or health condition that would be needed to be known by a medical emergency centre, user location.

It has to be discussed within the ongoing of the project if the following data will be stored:

- Medical info on disability.
- Name, address, tel, fax, e-mail, photo, etc. of the user (any direct or indirect link to user ID).
- Family members information.

### **3.2.2 During Preliminary Data Gathering (WP 2), Pilots (WP 3) and Training (WP 4)**

During the VERITAS Training sessions and Pilot tests:

1. Participants in the trials will give their names, address, and contact phone, together with age, gender, nationality and functional problem type (not medical term of disability!), to a single person in each pilot site, to be stored in a protected local database (to contact them and arrange for the tests). The contact person will issue a single Test ID for each of them. This person will not participate in the evaluation and will not know how each user behaved.
2. The names, address and contact phone will be kept in the database only for the duration of each trial (short term trials-up to 1 week, long term trials- up to 1 month). Such data will not be communicated to any other partner or even person in each pilot site. Once the test ends, they will be deleted.
3. Each month the anonymised data will be re-sorted randomly, to mix participants order.
4. Since personal data will be deleted, no follow-up studies with the same people will be feasible.
5. A local ethics pilot responsible will be named and trained (by the Ethical Manager/ COAT) in each pilot site or organisation which collects data, to monitor and guarantee that the relevant procedure is strictly followed and that all local Ethics Committee recommendations and national relevant laws are being respected.

## 4 Proposed Security issues in VERITAS

### 4.1 Introduction - the need for security

VERITAS aims to develop, validate and assess tools for built-in accessibility support at all stages of ICT and non-ICT product development, including specification, design, development and testing. The goal is to ensure that future products and services are being systematically designed for all people including those with disabilities and functional limitations as well as older people.

Thus, VERITAS system handles sensitive information that should be protected. The provision of VERITAS services requires a secure operational environment, and the project has dedicated to it sufficient resources and work (within WP3 and WP 4).

The level of security that should be included in the VERITAS system involves however some judgment about the dangers associated with the system and the resource implications of various means of avoiding or minimising those dangers. Several major questions arise, for example:

- How to safeguard the integrity of the information.
- How to safeguard the confidentiality of the information (i.e. who should be allowed to see what and under what conditions).
- How to improve its availability to legitimate users, etc.

In order to answer those questions it is necessary 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.

VERITAS information system is designed to provide the required level of security efficiently. However, as often happens, the objectives can conflict with each other. For example, security interests can conflict with performance. 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 that seem innocuous by themselves. Introducing security into VERITAS 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. This conflict will be dealt with in VERITAS by asking the user oneself to decide upon the accepted level of functionality and security one desires.

## 4.2 Fundamentals of VERITAS security and data privacy

VERITAS security and data privacy issues and layers are proposed in this chapter.

### 4.2.1 Main concepts

#### 4.2.1.1 Authentication

**Issue:** Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. It is a fundamental security requirement.

**State of the art:** In private and public computer networks (including the Internet), authentication is commonly done through the use of login passwords. Knowledge of the password is assumed to guarantee that the user is authentic. A second approach is to use something that users possess to present proof, such as a dedicated authenticator or smart card, special authentication software or a digital certificate. Still another approach to authentication utilizes biometrics — fingerprints, voice prints, retinal scans, etc. Two-factor authentication, which utilizes two of these approaches (e.g. password and authenticator), is generally considered the optimum way to ensure an adequate level of security.

**VERITAS specific demands:** Typical approach to authentication seems to be too complicated for mobility impaired and elderly. When testing the system or any device for example at home, SIM card based authentication and one more, easy-to-use additional method (e.g. PIN or biometrics depend on device capabilities) can be appropriate. Authentication type should be adjusted to user's disabilities. In any case, the generic public info module will operate without any need for authentication. Strict authentication rules will be introduced only for the VERITAS overall system operators.

#### 4.2.1.2 Authorization

**Issue & State of the art:** Authorization is the process of controlling what information, applications and services a user can access. Authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been already set up. Logically, authorization is preceded by authentication.

**VERITAS specific demands:** There is a strong demand for single, or reduced sign-on requirements, to minimize the number of times that authorized users need to authenticate themselves. As well as authentication, authorization should be adjusted to MI users disabilities.

#### 4.2.1.3 Confidentiality

**Issue:** Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security.

**State of the art:** Public networks typically don't support confidentiality with other means than the difficult access to the internal infrastructure. The access

can be further made difficult by the use of specific protocols, e.g. MPLS. In case of wireless networks, the shared medium (air interface) is protected by some encryption mechanisms which, however, proved to be not very difficult to break. In many application areas like health care, the level of confidentiality provided by the networks is not sufficient. The basic mechanisms of the network technology must be used, but in addition to this, end-to-end-security needs to be applied, typically by installing an IP-VPN.

**VERITAS specific demands:** VERITAS needs medium level of confidentiality. Specially, medical data must be secured from unauthorized access with highest priority.

#### 4.2.1.4 Anonymity

**Issue:** Anonymity assures that sensitive data cannot be associated with a particular individual, either from the data itself, or by combining the user transaction with other data.

**State of the art:** Nowadays many transactions that people undertake are entirely anonymous, including: barter transactions, visits to enquiry counters in government agencies and shops, telephone enquiries, cash transactions such as daily payments for inexpensive goods and services, gambling and road-tolls, etc.

**VERITAS specific demands:** It is very important to assure, that while collecting only a statistic data, no private information are being collected.

#### 4.2.1.5 Non-repudiation

**Issue:** Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

**State of the art:** In today's global economy, where face-to-face agreements are often not possible, non-repudiation is becoming extremely important to commerce. There are some solutions, which helps with obtaining non-repudiation:

- Digital signatures - unique identifier for an individual, much like a written signature.
- Confirmation services - the message transfer agent can create digital receipts to indicate that messages were sent and/or received.
- Timestamps - timestamps contain the date and time of document creation and proves that a document existed at a certain time.

**VERITAS specific demands:** Assuring of non-repudiation is very important in emergency scenarios (for example in the health domain). Responsible rescue center must not deny that an emergency alarm call was received.

#### 4.2.1.6 Accountability

**Issue:** For proper managing a VERITAS services (when testing the system at home), detecting denial of service attacks and dealing with inter-provider relations the VERITAS system needs to collect usage information indicating what kind of services were utilized, how long they were used – and in some cases – who used the services.

**State of the art:** Abdication of disclosure of personal information, including a person's real name, does not necessarily mean abdication of reliable and accountable transaction processing or a breach of legal compliance. On the contrary, even anonymous transactions can be accountable, if necessary.

**VERITAS specific demands:** Thanks to the technology, even when anonymous, people can still be accountable for their actions. For example, where identifiers are needed, pseudonyms can be used. Such pseudonyms may be linked to credentials that provide specific guarantees required by the VERITAS service provider. Moreover VERITAS users should be aware that they are responsible for maintaining the secrecy of their user ID and/or password/PIN, as well as all other proprietary security and access information, and possession of any security devices, such as authentication devices and smart cards.

#### 4.2.1.7 Integrity

**Issue:** Data Integrity assures that information stored on a system is reliable and can be trusted. Since systems are used to manage information, Data Integrity is a measure of the quality of that information. Most important factors of this measurement are: consistency, accuracy, and correctness of data stored in a database. Accordingly, it must be an integral part of VERITAS security module.

**State of the art:** Nowadays integrity of a data is assured at several levels of systems. There are specialized integrity constraints provided by every database management systems. Furthermore, it is important to proper design the user interfaces with relevant validation of input data.

**VERITAS specific demands:** Besides typical integrity requirements, VERITAS should provide a service assuring the recipient that any message was not modified during the transmission.

#### 4.2.1.8 Availability

**Issue:** VERITAS must provide services to its users according to a given policy. In general users should have rights giving them a guaranteed access to the services in case of emergency (only for automatic and health domain).

**State of the art:** In present systems there are several important factors, on which availability depends most.

**VERITAS specific demands:** VERITAS requires high level of availability (very high level means more than 99.5% of time - in 24/7 mode with less than 4 hours of monthly unavailability). Using of Failure Monitoring Systems constitutes thus

an urgent need, and it is quite important to assert redundancy of some physical components, DoS protection, and at least some simple DRP. Moreover, a malicious user should not be able to flood the system with malicious packets (for instance, attempt to create large numbers of sessions). Inside critical infrastructure the system needs a nearly 100% availability.

## 4.2.2 Security fundamentals

### 4.2.2.1 Cryptography

**Issue:** Cryptography is the study of mathematical techniques related to aspects of information security, such as confidentiality, data integrity, entity authentication, and data origin authentication. A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. It is also about the prevention and detection of cheating and other malicious activities.

**State of the art:** Cryptography includes techniques, such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear-text) into ciphertext (a process called encryption), then back again (known as decryption). Because some governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may pose a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. The European Union has played a key role in rejecting such restrictions on encryption. The European Commission requires Member States to report to the Commission any national proposals to impose technical rules for marketing, use, manufacture, or import of cryptographic products. The Commission also seeks to dismantle intra-Union controls on commercial encryption products.

**VERITAS specific demands:** VERITAS needs cryptography for securing private data, such as: position, health and medical data, user profile, etc. It will be also strongly engaged in e-services, such as e-payment and e-commerce. Despite these needs, there is no demand for any special or VERITAS-related modifications of actual cryptography technologies or solutions.

### 4.2.2.2 Security design

**Issue:** Any discussion of computer security necessarily starts from a statement of requirements, i.e., what it really means to call a computer system "secure". In general, secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, modify, create, or delete information. In "The Orange Book" ("security bible" provided by US Department of Defense) – there are presented six fundamental requirements, which are derived from this basic statement of objective:

- **Requirement 1 – Security Policy:** There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object. Computer systems of interest must enforce a mandatory security policy that can effectively implement access rules for handling sensitive (e.g., classified) information. These rules include requirements such as: No person lacking proper personnel security clearance shall obtain access to classified information. In addition, discretionary security controls are required to ensure that only selected users or groups of users may obtain access to data (e.g., based on a need-to-know).
- **Requirement 2 – Marking:** Access control labels must be associated with objects. In order to control access to information stored in a computer systems, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity level (e.g., classification), and/or the modes of access accorded those subjects who may potentially access the object.
- **Requirement 3 – Identification:** Individual subjects must be identified. Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with. This identification and authorization information must be securely maintained by the computer system and be associated with every active element that performs some security-relevant action in the system.
- **Requirement 4 – Accountability:** Audit information must be selectively kept and protected, so that actions affecting security can be traced to the responsible party. A trusted system must be able to record the occurrences of security-relevant events in an audit log. The capability to select the audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis. Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations.
- **Requirement 5 – Assurance:** The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above. In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions. These mechanisms are typically embedded in the operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such system mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency.
- **Requirement 6 - Continuous Protection:** The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes. No computer system can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion. The continuous protection requirement has direct implications throughout the computer system's life-cycle.

**State of the art:** At present, there are various tools designed to securing of computer systems. These are both software applications and hardware products. Based on them, many companies provide complex security solutions which secure software as well as hardware. Despite that, one of the most important thing is well-managed security policy. The developer of every VERITAS module should follow clues contained in this document (and prospective comprehensive Security Policy) to assure the security of the overall system.

**VERITAS specific demands:** Every VERITAS system module/ domain should be evaluated and marked with access control labels. Tracking in details every activity of user is very useful from a security point of view, but VERITAS cannot violate user's privacy. Audit methods should be clearly described. For every domain service, developer should provide specialized access / security policy, which extends main points included in present document as well as in prospective Security Policy.

#### 4.2.2.3 PKI Infrastructure

**Issue:** Public Key Infrastructure (PKI) included within the organization network system, and taken into account in its security policies is the basis, on which the confidence relationships between the organization and its clients or contractors can be built. Digital signatures ensure that the level of security for online transaction is as high as for the transactions closes in the traditional methods.

**State of the art:** In the public key infrastructure, the mechanism of confidence is based on so-called "third party". It can be a governmental institution, well-known company, or other well-know organization the society has confidence in. This party runs certificate authority - a unit responsible for issuing certificates that confirms the identity of users.

**VERITAS specific demands:** Procedure of gaining the certificate is quite complicated and it can be a problem for VERITAS user. Since we can assume that the user have PKI-key properly integrated in their devices or applications, we can profit of all PKI conveniences.

#### 4.2.2.4 Intrusion detection systems

**Issue:** An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

**State of the art:** There are several approaches to IDS challenge.

Misuse detection and anomaly detection: in misuse detection, the IDS analyses the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical

packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

Network-based and host-based systems: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.

Passive system and reactive system: in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

#### 4.2.2.5 Intrusion prevention systems

**Issue:** Intrusion prevention systems are proactive defence mechanisms, designed to detect malicious packets within normal network traffic (something that the current breed of firewalls do not actually do, for example) and stop intrusions, dead blocking the offending traffic automatically, before it does any damage, rather than simply raising an alert as, or after, the malicious payload has been delivered.

**State of the art:** Within the IPS market place, there are two main categories of product: Host IPS and Network IPS.

#### 4.2.2.6 Central logs

**Issue:** Collecting of all system's logs in one central place strongly improves the processes of system administration. Such logs can be easily stored and archived. It's also possible to correlate various events from different systems. Moreover, system administrator can read the logs from certain system, even after system crash or hacker's interpose.

**State of the art:** Usually central logs system consists of two main types of elements – agents and manager.

**VERITAS specific demands:** The idea of central logs cannot be strictly applied to the whole VERITAS system, since there is not planned any central server or repository. Though, when considering VERITAS Intelligent system architecture as the basic medium, which integrates and interconnects numerous devices, sensors and agents, it may be sensible to create central logs service for such scope.

#### 4.2.2.7 Failure monitoring systems (FMS)

**Issue:** Continuous monitoring functionality, provided by failure monitoring systems, is one of the most important parts of assuring system's high availability. Aim of failure monitoring systems is to properly track failures, and then, immediately notify the responsible subjects.

**State of the art:** Failure monitoring systems can rely on different solutions. One of the most popular approaches is to expose outside ordinary database procedures. Monitored system should call those procedures when an incident

occurs. We can distinguish two main types of alarms: static and dynamic. Static alarm usually has own static ID, and can be switched on or off. This switching can be realized in few ways. It can be simple on/off switching or it can rely on counters or timers. Properly set values of timers and counters thresholds are big challenge for system integrator, because wrong values can rise to deceitful system's status or system's overload. Dynamic alarms are reported only once and with dynamically generated ID. They can not be switched off.

**VERITAS specific demands:** For some VERITAS scenarios there is a need of continuous systems monitoring. In emergency use-cases, user's health and life can directly depend on one's service availability. Hence, the need of immediate alarm is obvious.

## 5 Applied privacy issues

### 5.1 General principles

Personal information must be regarded as confidential. Normally custodian of a large research database or register must ensure they have each persons' explicit consent to obtain, hold and use personal information.

The following aspects of privacy will be strongly taken into account by all researchers when handling (pre-processing, storing, distribution, etc.) personal data:

- **Hints** to or specific personal information of any participant in publications. It is prevented within VERITAS to reveal the *identity* of participants in research deliberately or inadvertently, without the expressed permission of the participants.
- **Dissemination** of data among partners.
- **Access** to data. Define and protect method of access, data formats, method of archiving (electronic and paper), including data handling, data analyses, and research communications. Offer restricted access to privacy sensitive information within the organization of the partner.
- **Protection** of the privacy within the organization of volunteers (employers, etc.) throughout the whole process like, communications, data exchange, presentation of findings, etc.

Furthermore, the participants have to be able to control the dissemination of the collected data. The investigator is not allowed to circulate information without *anonymisation*. This means that only relevant attributes, i.e. gender, age, etc. are retained. Personal information (e.g. identity, etc.) will be stored by one designated person in each site (in a password protected file), only for the duration of the test of each user and will then be deleted.

While common law establishes some core principles, it does not specify when confidential information may be disclosed to others, in research. Individuals and organizations using confidential information have to take responsibility for deciding what is justified and acceptable also on a case by case basis (Medical Research Council, 2000).

As already mentioned, protection of confidentiality implies informing the participants about what may be done with their data (i.e. data sharing). Within VERITAS all research participants will be clearly informed about privacy aspects as listed in the 'VERITAS informed consent template concerning private information' that can be found in the annex.

As databases are developed, confidentiality will become increasingly hard to maintain. Simple stripping of the participants name and its replacement with a code is no guarantee of complete confidentiality.

The Ethics Advisory Board will especially scrutinise the information preprocessing within databases.

A question currently under debate among behavioural scientists is whether a consent form stating that personal data will not be shared precludes sharing of data even if identifying characteristics are removed. The removal of identifying information from data gathered on an individual may not be enough, since identities can be reconstructed from disparate data sources.

Within VERITAS the participant will be informed about the sharing of his/her data, even, if only anonymised data is being shared.

There are solutions to the challenge of maintaining confidentiality including substituting numerical identifiers for names, aggregating data so that the performance of individuals is not obtainable, encryption or layering data so that researchers who need identifying information can obtain it only after signing a legal document that requires honouring the confidentiality of individuals.

VERITAS has thus decided that:

1. All research using identifiable personal information, or using anonymised data which is not already in the public domain, must be approved by a Research Ethics Committee.
2. All personal data must be coded or anonymised as far as is possible and consistent with the needs of the study, and as early as possible in the data processing. Only personal identifiers that are essential should be held.
3. Each individual entrusted with personal information is personally responsible for their decisions about disclosing it.
4. Pilot site managers must ensure that personal information is handled only by staff with an equivalent duty of confidentiality.
5. Pilot site managers (see chapter 8) must take personal responsibility for ensuring that training, procedures, supervision, and data security arrangements are sufficient to prevent unauthorized breaches of confidentiality.

All the above principles are in accordance to Medical Research Council (2000).

## 5.2 Anonymisation and Coding

Information should be anonymised so that individual identities cannot be revealed. Anonymisation provides a safeguard against accidental or mischievous release of confidential information.

There are different ways in which personal data can be modified to conceal identities:

**Coded information** contains information which could readily identify people, but their identity is concealed by coding. The key to which is held by members of the research team using the information.

**Anonymised data with links** to personal information is anonymised to the research team that holds it, but contains coded information which could be used to identify people. The key to the code might be held by the custodians of a larger research database.

**Unlinked anonymised data** contains nothing that has reasonable potential to be used by anyone to identify individuals.

As a minimum *anonymised data* must not contain any of the following, or codes for the following:

- Name, address, phone/fax. Number, e-mail address, full postcode.
- Any identifying reference numbers.
- Photograph or names of relatives.

With both linked and unlinked anonymised data it is sometimes possible to deduce individuals identities through combinations of information. The most important identifiers are:

- The *age*, if a small sample size is taken; in this case there has to be compromised between scientifically precision and the protection of the individual privacy.
- Rare disease or treatment, especially if an easily noticed illness is involved.
- Partial post-code, or partial address.
- Place of treatment.
- Rare occupation or place of work.
- Combinations of birth date, ethnicity, place of birth, and date of death.

Researcher and database developer will always consider – when designing studies, before passing information to others, and before publishing information- whether data contain combinations of such information that might lead to identification of individuals or very small groups. How much of this potentially identifying information can be safely included in data that is assumed to be unidentifiable can only be judged on a case by case basis taking into account the sample size, the ways in which results will be published and used (Medical Research Council, 2000).

Within VERITAS we will follow the ***unlinked anonymised data policy***, excluding users having rare diseases and any other identifiers, except ***type of impairment*** (as category only, not with medical detail), ***age, gender and nationality***. Once anonymised, the data will not allow tracing back the participant in any way. Other databases of participants will not be maintained, neither centrally nor locally.

### 5.3 International and European instruments in the field of data protection

The Council's of Europe Convention for the protection of individuals with regard to automatic processing of personal data is the first European instrument in this field. It laid 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. Art. 6 states that medical data may not be processed automatically unless domestic law provides appropriate safeguards. The Convention is of limited importance for EU countries after the enactment of the EC Directives on data protection.

The Charter of Fundamental Rights in the course independent authority 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 based on the consent of the data subject or other legitimate basis set 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 which shall control the compliance with the data protection rules.

In 1999 the Council of Europe has adopted the Recommendation 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 OECD 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. Although the Recommendation does not address healthcare applications, its provisions might apply as following:

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. click streams or purchased profiles.

### 5.3.1 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 regulates the processing of personal data, regardless if the processing is automated or not.

#### **Scope**

Personal data is defined as "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/her physical, physiological, mental, economic, cultural or social identity;" (art. 2 a).

This definition is meant to be very broad. Data is "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of "personal data": address, credit card number, bank statements, criminal record, ...

The notion *processing* means "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;" (art. 2 b).

The responsibility for compliance rests on the shoulders of the "controller", meaning the natural or artificial 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; (art. 2 d)

The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. (art. 4) Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any on line shop trading with EU citizens will process some personal data and is using equipment in the EU to process the data (the customers computer). As a consequence, the website operator would have to comply with the European data protection rules. The directive was written before the breakthrough of the Internet, and to date there is little jurisprudence on this subject.

### **Principles**

Personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose and proportionality.

#### **- Transparency**

The data subject has the right to be informed when his personal data are being processed. The controller must provide his/her name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair (art. 10 and 11).

Data may be processed only under the following circumstances (art. 7):

- when the data subject has given his/her consent;
- when the processing is necessary for the performance of or the entering into a contract;
- when processing is necessary for compliance with a legal obligation;
- when processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

The data subject has the right to access all data processed about him/her. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules (art. 12).

#### **- Legitimate Purpose**

Personal data can only be processed for specified, explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes (art. 6 b).

- **Proportionality**

Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use (art. 6).

When sensitive data is being processed, extra restrictions apply (art. 8). The data subject may object at any time to the processing of personal data for the purpose of direct marketing (art. 14).

A decision which produces legal effects or significantly affects the data subject may not be based solely on automated processing of data (art. 15). A form of appeal should be provided when automatic decision making processes are used.

**Supervisory authority and the public register of processing operations**

Each member state must set up a supervisory authority, an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection regulation has been violated. (art. 28) Individuals may lodge complaints about violations to the supervisory authority or in a court of law.

The controller must notify the supervisory authority before he/she starts to process data. The notification contains at least the following information (art. 19):

- the name and address of the controller and of his/her representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;
- proposed transfers of data to third countries;
- a general description of the measures taken to ensure security of processing.

This information is kept in a public register.

### 5.3.2 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.

### **5.3.3 Art. 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 EC Directives and International Agreements will be fully adopted within VERITAS. The conformance to them will be safeguarded by the VERITAS Ethics Advisory Board.

## 6 Risk assessment, delegation of control, deception and debriefing

Life without computers is unimaginable for most of us today – embedded processors monitor the condition of high risk – patients around the clock, they control central heating in buildings, air conditioning in tunnels, and airplanes are safely guided... The potential economic benefits of ubiquitous computing and VR development are certainly key factors for the further proliferation of these techniques.

On the other hand, the Ethics Advisory Board will scrutinise the research that no undue risk for the user whether technically, nor related to the breach of privacy is possible. But it is not possible to conceive a procedure, investigation, or process which would be without any risk. One of the most important factors in the assessment of risk is the perception of the prospective participant of the importance of risk. The participant's life situation may substantially influence the way in which a risk is perceived. The end point of the process is the consent 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 – is given to the participants. This means that the project *VERITAS 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.

There will be possibilities to ask questions, detailed information also under Chapter Informed consent.

Categories of risk:

- There will be no risk of physical damage within the experiments taken in VERITAS. Any equipment connected to a participant will be evaluated for personal safety. These tests will be performed for the complete configuration and not only for the individual equipment.
- Psychological consequences will be carefully examined.
- Social inconveniences will be minimised (no additional stress for families, cost reimbursement for additional transportation costs, ...).
- If private information is recorded, the participant will be informed according to the aspects mentioned in the informed consent template concerning privacy.
- The Security of the IT infrastructure and the Privacy related information concerning the risks is described in the corresponding chapters.
- ***In case any user might be endangered by inappropriate information, he/she shall be supervised during the pilot and training tests by a experienced supervisor.***

## 6.1 Aml Control level vs person's control level

In order to minimize the need for human intervention in complex, highly dynamic environments, new concepts for delegating control are often necessary.

Different aspects can be summarized.

- **Content control:** If smart objects provide information about themselves, this raises the question of who guarantees the objectivity and accuracy of the statements made. The content of developed VERITAS objects will be continuously checked.
- **System control:** The objectivity, reliability and objectivity of the system functioning is to be guaranteed. The system of the developed VERITAS will be continuously checked.
- **Accountability:** If autonomous objects start taking decisions on their own, legal guidelines need to be drawn up, in order to resolve who is ultimately responsible these decisions taken [Bohn et al., 2005].

The ambient intelligent technology has a *high control level*, when it acts on behalf of a person, e.g. it rejects an action on behalf of a person.

Ambient intelligent technology has a *medium control level*, when it gives advice; e.g. to reduce car speed due to a road bend ahead.

Ambient intelligent technology has a *low control level*, when it only executes a persons command.

As devices for user groups with different handicaps are developed, the user will be given an aid to compensate the deficiency. But there is also a certain danger that the user will loose autonomy. This loss of personal control will be carefully checked.

Research will carefully be controlled, that the users have a high control on all developed products and services, so the dependability on technical devices will be held as low as possible. This could be achieved as follows (especially important for the healthcare domain): *Note: the next bullet points have to be regarded as proposition*

- ***The user will select if he/she accepts the system to monitor his/her behaviour, disabling the monitoring module (working space/ domotics/ healthcare due to his/her special need) once and for all or in specific instances.***
- ***When the monitoring module is on and monitoring user actions, constant feedback (i.e. by LED or other) will be given to the user.***
- ***The user will be able to access his/her static and dynamic profile, delete or alter it, using a personal password.***

## 6.2 Deception

Researchers do not conduct a study involving deception unless that they have determined that the use of deceptive techniques is justified by the study's significant prospective scientific, educational, or applied value and that effective non-deceptive alternative procedures are not feasible. Researchers do not deceive prospective participants about research that is reasonably expected to cause physical pain or severe emotional distress.

Researchers explain any deception that is an integral feature of the design and conduct of an experiment to participants as early as feasible, preferably at the conclusion of their participation, but no later than at the conclusion of the data collection, and permit participants to withdraw their data (American Psychological Association, 2002).

No deception will take place within VERITAS pilots. It is not decided that maybe in a few trials the system functionality will be emulated by a hidden evaluator (WoZ trials), without the user knowing that the system is not yet operative. But this is of no importance to the user and will be communicated to him/her after the end of the test. Such trials will be performed only for early recognition of user needs, before a system prototype is available.

### 6.3 Debriefing

Researchers provide a prompt opportunity for participants to obtain appropriate information about the nature, results and conclusions of the research, and they take reasonable steps to correct any misconceptions that participants may have of which the researchers are aware (American Psychological Association, 2002).

**Participant can decide** if researchers inform the participants about symptoms or diagnoses of diseases that have been discovered during the study (where medical doctors and psychologist test participant ); especially if the symptoms have not discovered yet by a physician. Relevant test results will be provided to participants General Practitioner (see also section 3.1).

Within VERITAS, if tests point strongly to a participants incapability (i.e. revealing significant mental or cognitive problems not known before), the participants will be informed hereof and advised to undergo further testing and examination by a medical / psychological traffic expert of his / her choosing (driving domain).

The debriefing has to be documented and will be signed by both sides. Summaries and copies of research reports will be given to research participants in appropriate accessible formats (e.g. \*.pdf, html, printed, in Braille oral communication, etc.). They will not be communicated to any authority or third party.

## 7 Organization and insurance issues

All partners are obliged to respect the user's privacy, informed consent as well as the safety requirements. They should be aware of risks involved while conducting the studies. The consequences of risks are to be borne by the partner individually and not to be shared with the project or other partners. Appropriate insurance or indemnity to cover the participant in a trial should be provided according to the regulations of the Local Research Ethics Committee (LREC). In any case the VERITAS Ethics Advisory Board recommends insuring the participants.

### 7.1 Ethics control committee

Any organization performing experimental work with human beings or animals must have an ethics control committee (even a local panel within the organisation, or an LREC = Local research Ethics Committee) that must evaluate all the aspects mentioned here and formally approve the experimental procedures.

### 7.2 Accessibility of Facilities and Services

It is unlawful to discriminate against disabled people by refusing them access to services or providing a lower standard of service. There are also laws that require service providers to make reasonable adjustments to the way they provide their goods, facilities and services to make them accessible to disabled people. In this respect, it is the responsibility of each partner of VERITAS Consortium to ensure that contractors follow these steps for the disabled people involved in the VERITAS research:

- In organising any workshop, presentation or focus group, people who are invited are asked if they require special facilities, for example, signers and/or amplification.
- Buildings and rooms must be accessible for all types of MI users considered within VERITAS.
- Use of small typefaces should be avoided. In printed material, 14-point type is preferable (e.g. copies of handouts); on screen presentations should be clearly legible.

### 7.3 Reimbursement Schemes

#### 7.3.1 Incentives for research respondents

Payment of incentives to research respondents should be considered in return for participation. Participants should not normally be paid for participation in standard cross-sectional surveys, primarily because of large sample sizes and the large cost involved. There is also a danger of creating an 'incentives culture' if payment is expected for participation in all research, although the VERITAS partners are aware of the increasing difficulties in recruiting respondents. However, incentives should be considered where the research is particularly onerous, for example, a very long survey interview (beyond the average 45-60

minutes), for most qualitative research (face-to-face interviews, diary completion or group interviews where attendance is crucial and timing inflexible for the individual), or an ongoing commitment to a survey series.

Incentives should not normally be paid to respondents who are being interviewed in their professional capacity. Instead, they may need to be recruited through their employer and the involved VERITAS partners should normally seek to gain their executive's permission to conduct the research during working hours. There may, however, be instances where it is appropriate to pay incentives to certain research groups.

### **7.3.2 Legal basis for reimbursements as incentives**

Generally, legal basis for paying incentives to benefit recipients without affecting benefit payments may be interpreted as such:

Small one-off payments (say 20-30 €) to benefit claimants can be paid because they should be treated as capital rather than income. However, larger sums of funds constitute remunerative work, so it could affect all types of customers' benefit and better be avoided. But in any case, different practices may be applied in different Member States, and this should be examined.

Normally remunerative work would affect a customer's entitlement to benefit if they worked above a threshold (16-20) hours a week; if they worked less hours than the threshold per week, it may affect the amount of benefit they receive if they earned more than their earnings (it is possible, in some cases and in some member states, interviewees are allowed to earn the reimbursement amount of their participation in the VERITAS research, without these earnings to being taken into account in the calculation of their benefit). In these cases, the involved VERITAS partner should assess whether participation affects ability to work and whether participation in a given research affects their normal benefit provided by the state in order to be taken into consideration and to be avoided.

Therefore, in the cases where reimbursement incentive is foreseen, claimants (research interviewees) should be made aware of the status of the payment in opt-out letters using the following terminology: 'If you do take part in the face-to-face discussion, you will receive XX € in cash, as a 'thank-you' gift for your help with this study. This will not affect your entitlements to benefit in any way.'

If an involved VERITAS partner is ever in any doubt about a legal issue, he/she should refer it to its legal services and inform the VERITAS Ethics Advisory Board.

### **7.3.3 The amount to pay**

Legal ethical advice suggests clearly that payments should be small and a one-off. The VERITAS partners involved should pay the same amount of money to each of its respondents. Previous practice suggests that, where it is appropriate to pay respondents incentives, new contracts could be established that pay roughly 15€ for a survey interview, 20€ to participants for in-depth face-to-face interviews, 25€ for focus groups and 50€ for a day long 'workshop' or trial. However, this preliminary guidance will need to be reviewed by the involved VERITAS partners.

### **7.3.4 Type of payment**

Respondents can be paid in cash or with a gift voucher. The advantages of vouchers are that on the one hand they may be more suitable for vulnerable groups, such as 'chaotic' drug users or alcohol abuser (although this is not the case in VERITAS), and on the other hand interviewers may feel more comfortable carrying them. It is also good practice when conducting research to use vouchers for incentive payments.

The advantages of cash are that it does not compromise the VERITAS partner's neutrality if particular organisations' vouchers are given and also cash may be more useful to benefit recipients. Respondents should be paid after the interview/trial and a record of the payment received kept by the researcher. VERITAS partners involved are expected to use their discretion to decide the most appropriate method of payment.

## 8 Ethical issues across the project life-cycle

VERITAS is a large and complex project with ethical issues related to security, privacy and accessibility. Each phase of the project will be accordingly addressed from the project concept development to the project closure.

The following issues are identified as core ethical issues: privacy protection and confidentiality, Informed consent, transparency of the data management, appropriate IT-security and identity management to ensure privacy of personal data, risk assessment and delegation of control. It is possible that in this highly innovative research field, additional ethical issues will be identified during the project. Therefore official documents, such as this Deliverable, will be revised according to the comments of the partner reviewers and ethical board members. Different instances (such as the Ethics Advisory Board, COAT and all other (data collecting) partners will supervise all studies and pilots supported by a local research ethics committee.

### 8.1 Methodology

A questionnaire has been developed and circulated to all partners, so as to collect practices and legislation in the various countries regarding the issues above. It is included in the Annex I: 'Questionnaire on ethical and legal issues'.

The objectives are to collect the nationally or organisationally adapted ethical issues mentioned in this manual, as per local usages of LREC.

All the issues mentioned in this manual are picked out as a central theme in the questionnaire on ethical and legal issues. The purpose is to collect information from the VERITAS partners who are planning to conduct pilots, training or studies, but it has also an educative function: to point the partners the relevant ethical issues that are described in this ethics manual.

Yet it is too early to summarise the results that will be gathered with the above mentioned document (questionnaire on ethical and legal issues). In the final form of the manual a relevant summary will be given.

CHECKLIST before the Pilots/Training/study begins:

1. Fill in ANNEX 1 – 3 and 8 and send it to Ethical secretary (COAT-Basel)
  - The Ethical secretary will send it to the Ethics Advisory Board
  - In second step the Ethical secretary will provide feedback due to the panels` comments
2. Send pilot/training/study plans to Ethical secretary (COAT Basel)
  - The Ethical secretary will send it to the Ethics Advisory Board
  - In second step the Ethical secretary will provide feedback due to the boards` comments
3. Send pilot/training/study plans to the LREC (wait for the approval!).
4. Conduct the pilot (Informed Consent included)
5. Evaluate the pilot from a final point of view regarding the ethical issues and send feedback to COAT.

## 8.2 VERITAS Ethics Advisory Board

All used assessment tools and protocols within VERITAS Pilots will be verified beforehand by its **Ethics Advisory Board**, regarding their impact to users' well-being before being applied to the pilot sites. Two renowned experts in the field, chaired by an experienced ethics coach, constitute the project Ethics Advisory Panel, assisted by further external experts, when needed. The Ethics Advisory Panel assumes responsibility for implementing and managing the ethical and legal issues of all procedures in the project, ensuring that each of the partners provides the necessary participation in VERITAS and its code of conduct towards the participants. All relevant liaisons with the Commission will be through the secretary ethics advisory Panel.

The Ethics Advisory Board of VERITAS consists of the following persons:

- Prof. Dr. V. Dittmann, Director of the Institute for Forensic Medicine of University of Basel.
- Prof. Dr. Jürgen Maes, Universität der Bundeswehr München, Vertreter der Professur für Pädagogische Psychologie unter besonderer Berücksichtigung der Lernpsychologie; Werner-Heisenberg-Weg 39  
85577 Neubiberg  
Tel.: 089-60043154  
URL: <http://www.unibw.de/paed/psy>

### Secretary of the Ethics Advisory Board:

Marcel Delahaye  
COAT-Basel  
Wilhelm-Klein-Str. 27  
4025 Basel, Switzerland  
Tel. +41 (0) 61 325 57 61  
Fax. + 41 (0) 61 383 28 18

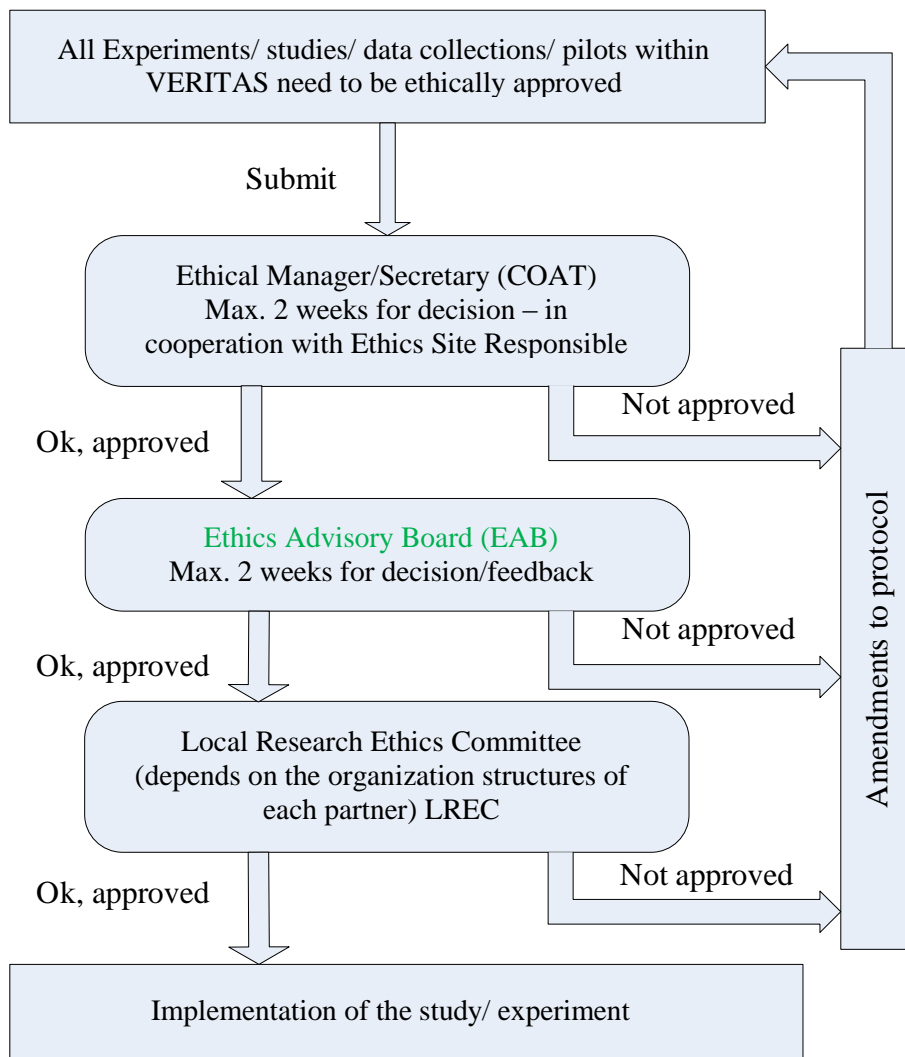
E-Mail: [key@coat-basel.com](mailto:key@coat-basel.com)

Drawing on the basic philosophies underlying major codes, declarations, and other documents relevant to research with human subjects, the Ethical Secretary proposes 11 requirements that systematically elucidate a coherent framework for Ethics for Research and Dissemination:

- 1) Value: enhancements of health or knowledge must be derived from the research;
- 2) Scientific validity: the research must be methodologically rigorous;
- 3) Fair subject selection: scientific objectives, not vulnerability or privilege, should determine communities selected as study sites and the inclusion criteria for individual subjects;
- 4) Favourable risk-benefit ratio: within the context of standard clinical practice and the research protocol, risks must be minimized, potential benefits enhanced, and the potential benefits to individuals and knowledge gained for society must outweigh the risks;
- 5) Independent review: unaffiliated individuals (e.g. Ethics Advisory Board) must review the research and approve, amend, or terminate it;

- 6) Informed consent: individuals should be informed about the research and provide their voluntary consent;
- 7) Respect for enrolled subjects: subjects should have their privacy protected, the opportunity to withdraw, and their well-being monitored;
- 8) Establish the investigators assuming responsibility for results dissemination (data, anonymisation, true reporting);
- 9) Ascertain the means by which the investigators propose to disseminate the research results;
- 10) Scrutinise any sponsor-imposed contractual impediments to results dissemination;
- 11) Mandate trial registration;

Fulfilling all 11 requirements is necessary and sufficient to make (clinical) research and dissemination ethical. These requirements are universal, although they must be adapted to the health, economic, cultural, and technological conditions in which clinical research within VERITAS is conducted. One of the major topics of the Ethics Advisory Board is to safeguard these issues. The following flow chart gives an overview about the procedure of the Ethical Management in general (including the **Ethics Advisory Board**).



**Figure 1: Ethical Management procedure.**

### 8.3 Explanation

All Experiments, studies, data collections, pilots within VERITAS need to be ethically approved. At first, the VERITAS Ethical Manager/Secretary (COAT) has to decide whether the provided documents are compliant considering the ethics legislation. The Ethical Manager works in close cooperation with the Ethics Site responsible (see table below). After having passed this step, the required documents will be reviewed by the External Ethics Advisory Board of VERITAS (EAB). These two steps should take no more than two weeks per each VERITAS advisory level (secretary and EAB). If having been approved by the Ethical secretary and the EAB, the documents will be sent to the specific local research ethical committee by each partner. If the study/ experiment/ pilot is also successfully approved by this, its performance can take place. If there are any doubts by any authority (Ethical Manager, EAB or Local Ethical Research Committee), the experiment's design has to be changed to get the final approval. All amendments have to be approved again not only by the authority which refused to approve the experiment, but also from all authorities which have already given green light. Once the local application had been accepted a copy of the relevant document will be collected by the Ethical secretary. All collected ethical approvals will be kept in a separate file and are available for ethical review by the EU commission, external reviewers and the Ethical Advisory Boards on request.

Each data collecting site (Pilot, Experiment, etc.) is going to prepare an ethical advisory board application (see ANNEX IX).

This includes

- The actual application/pilot description
- Case Report form
- Informed Consent
- Sponsor Information; in this case the EU
- Insurance for healthy volunteers

As stated in this Ethics Manual, before any data collection will start, all data collecting partner have to fill out ANNEX I and ANNEX VIII of the Ethics Manual. Both will be sent to the Ethics Advisory board by the Secretary in order to get their approval. These steps shall raise the awareness of the VERITAS partners for Ethical Issues. So far we received feedback from: UNEW, CRF, MCA, UPM ,FHG and BYTE.

### 8.4 Clarification of the role of the Ethics Advisory board (EAB)

The EAB has been set up by COAT. The candidates have been picked due to their Academic background. These members will report their comments and these will be included, together with partners' feedback, and the emanating Deliverable changes will be added – if necessary – in the project pilot plans Deliverable (final version).

All assessment tools and protocols within VERITAS experiments, studies, data collection and pilots will be submitted for review to the Ethical Manager/Secretary (COAT) and the Ethics Advisory Board, before being applied to the Local Research Ethics Committees. The EAB will evaluate project

impact to user's welfare, respect for fundamental human rights and compliance with European ethical and privacy standards. Special attention will be given to design and plan the applications within VERITAS in accordance to national and European laws. In case of consistent problems with any of the initial pilots, a replacement of these applications in a laboratory environment with similar conditions is foreseen. The final decisions of the Ethical Manager and the EAB will be pointed out in the different Controlling Reports:

- D4.1.3: First ethical controlling report month 18;
- D4.1.4: Second ethical controlling report, month 36;
- D4.1.5: Ethics Manual-revised version, month 48

and will be communicated in individual emails to the SP3 and SP4 partners if needed. Special attention will be given to the confidentiality of data storage and processing. VERITAS partners have to document their data protection standards in ANNEX I of the Ethical Manual, which will be checked by the EAB. The EAB does not substitute any national or local ethical committee but supports their work by reviewing all procedures involving human subjects within VERITAS.

The EAB meets at least once a year and any time if it is necessary; it is envisaged that most work will be done via email and call conferences. EAB meetings are convened by the Ethical Manager who also sets the agenda. Brief minutes will be circulated to the VERITAS steering group and if necessary directly to the respective partners. **There is no direct contact foreseen between the partners and the EAB.** Members of the EAB are not compensated but they are fully reimbursed for their travel and lodging expenses. The EAB takes its decision by consensus. If consensus cannot be reached, a minority report will be attached to the issued advice. The role of the Ethical Manager/ Secretary is only on a mediation level between the two board members.

## 8.5 EAB terms of reference

The VERITAS Ethical Advisory Board (EAB)'s terms of reference are the following:

- to evaluate VERITAS impact to end users welfare (designers & especially elderly and disabled persons),
- to monitor the respect for fundamental human rights and compliance with European ethical and privacy standards during any data collection, study or pilot involving human subjects
- to approve research protocols and informed consent procedures and forms
- to support Local Research Ethical Committees (if needed)
- ensuring that each partner strictly adheres to the highest privacy and ethical standards

Therefore the EAB together with the Ethical Manager/Secretary will safeguard the performance and set up of the pilots (SP3), and the training of different end user groups (SP4), as well as the preliminary user feedback in SP2. By reading and commenting on the respective Reports and Deliverables, the comfort and safety of all participants has to be guaranteed, as well as the security and legal

issues of their personal data (e.g. related to their special needs and preferences). Relevant Deliverables for the methodology are D1.1.2 “UCD design guidelines for applications development”, as well as D3.6.1 “Pilot Planning and Evaluation Framework”, and both Deliverables in WP 3.7 and D3.8.1 will be checked by the Ethics Advisory Board.

The EAB will also keep an eye on the project developments as a whole, in a way that guarantees that future products and services are being ethically designed for all people including those with disabilities and avoids the creation of barriers, as well as the protection of their personal data (health status, capacities, abilities, location, routing, etc.)

EAB's outcomes are:

1) Minutes

2) Opinions

ad 1): Minutes of each meeting will be taken by the Ethical Manager/ Secretary. Finally they will be included in the Ethics controlling reports and the relevant partners will be contacted if any Ethical issues arise during the meetings. As a general rule they are restricted.

ad 2) Opinions are usually approved by consensus, when a consensus is not reachable a minority report will be included. They may concern both a specific issue raised by the project or a general ethical questions related to any activity which is of relevance for the project. They may be issued under request of a project partner or may be initiated autonomously by the EAB.

In order to get a closer look to the ethics code of conduct of research within VERITAS I referre to the relevant chapters of Ethics Manual at hand. Within this document, the key ethical and legal issues are identified and a relevant project policy towards examining these issues is developed.

In general it is the code of conduct for the project, that all project partners' Deliverables and pilots conduct will be scanned on behalf of the information listed in this manual. Relevant international and European conventions (e.g. Helsinki Declaration) are fully integrated in this manual. In the course of the project, also all national legislations will be fully integrated (e. g. Ethical approval for the pilots). In utilising the 'Template on ethical and legal issues' (ANNEX I) for those partners conducting training, pilots, or any kind of data collection, specific national standards and local conventions of ethics committees are being scanned and integrated.

All in all, this manual is conceptualised to offer guidelines for all research performed within the auspices of VERITAS.

## 8.6 Ethics Site Responsible

All European Union member states have a new legislation on clinical research after the implementation in their national laws of a Brussels' directive of 2001 (European Parliament. Directive 2001/20/EC of the European Parliament and Council of 4 April 2001. Official Journal 2001; L121:34–44); which became effective in 2004 (Silverman HJ, Druml C, Lemaire F, Nelson R. The European Union Directive and the protection of incapacitated subjects in research: an

ethical analysis. Intensive Care Med 2004; 2004:1723–1729) and which makes submission of research protocols to ethics committees mandatory. However, in most of the EU countries, these new legal requirements deal only with research on drugs and clinical studies. Nevertheless all data gathering activities within VERITAS have to be approved due to their ethical impact.

With regard to the importance of Ethical Issues, the most feasible approach in order to safeguard the Ethical Code of Conduct, at each data collecting site, a person has been nominated, who is responsible for ethics safeguard:

Site	Domain	Ethical Issues/ data protection (ethics site responsible)
COAT Basel	Infotainment pilots VR/AR games	Marcel Delahaye WP 3.8.1/5
UNEW	Infotainment pilots Pilot planning and framework	WP 3.8.1/5 Amy Wong
CRF	Automotive pilots - Accessibility of interior equipment for passenger vehicles to older people and users with physical / cognitive impairment Usability of IVIS HMI featuring different modalities (including vocal interaction) - Usability of IVIS HMI featuring different modalities (including vocal interaction)	WP 3.8.2 Dr. Ing. Guiseppa Varalda
BAUUNION	Smart living Spaces Accessible houses, focus on kitchen and bathroom	WP 3.8.3 Andreas Schurig
CAF	Automotive pilots ADAS/IVIS	Dr. Serge Boverie
PIAGGIO	Automotive pilots Interface design for PIAGGIO	Mr. Mario Santucci
FhG	Conducting the pilot tests with developers and designers	Tim Gleue
Hypertech	Office workplace Ergonomic & accessible design of workspace	Mr Thomas Papapolyzos
MCA	Infotainment pilots Accessible interfaces (physical and cognitive)	C. van Isacker
FIMI (to be replaced – left the project)	Healthcare domain - Older people with cardiovascular diseases - Older people with some kind of physical impairment	Dr. Silvio Bonfiglio (left the project)
INDESIT	Smart living Spaces White goods	Renato Aiello
BYTE	Office workplace Communication aids for blind/deaf	WP 3.8.4 Nikolas Bezerianos

**Table 4 Partners responsible for ethics safeguard.**

To assure the above described way on how to get ethical approval for each experiment, study, data collection or pilot being performed within VERITAS project, each data collecting partner is going to nominate an ethics responsible. He/She has to take care about

- Ethical Protocol
- Informed Consent
- Data management
- Sponsor Information; in this case the EU
- Insurance for healthy volunteers
- Contact person for the Ethical Secretary and Ethical Advisory Board

This persons are mainly in charge of the data collection during the pilots: within the scope of VERITAS, two different pilot sets are involved.

First, the **pilots for developers and designers** will be organized at 4 pilot sites countries (Germany, Greece, Italy, UK) (see WP3.7): at the end of the 2nd year and during the 3rd year and will involve 140 developers/designers. The piloting will consist of iterative evaluation and testing cycles.

Second, the **pilots for the end-user, also called beneficiaries** (people with disabilities and older people) will take place at 5 pilot sites (Belgium, Bulgaria, Italy, Greece and the UK). Within the scope of VERITAS, 380 participants will be tested.

Before each pilot of VERITAS' five application fields will be preceded by a dedicated demo event during which the local pilot users will be able to get themselves accustomed with VERITAS tools. In addition Ethical responsables will receive a special ethical tutoring (containing: informed consent, data protection, special needs of the end-users, etc.). The end-user groups are: Blind and low-vision users, Motor impairment users, Cognitive impairment users, Hearing impairment users and speech impairment users. The relevant WP for end-user and impaired participants is WP3.8.

## 8.7 VERITAS Ethics Control at the Pilot and training Sites

As already mentioned in section 3.3.2 , an Ethics Site Responsible will be identified in each pilot site, to guarantee that the pilots abide to the overall VERITAS Ethical Policy; relevant approach will be given by the local research ethics committees and the local data stored on test subjects are kept properly secure and anonymised before use. This role per site has been given to the following persons/organisations:



**Tab 1: Preliminary selection of Ethical issues and data protection responsables per VERITAS pilot site WILL BE COMPLETED IN A LATER STAGE OF THE PROJECT, as the final pilot partners (designers) and end user organisations are not specified yet (Month 5).**

### 8.7.1 Workshop for the Pilot sites

After the Identification and recruitment of an ethics expert for data protection, (a named person locally responsible for ethical matters and data protection at each site) (See above) a workshop will be hold in one of the next meetings of the project, to provide the responsible partners with relevant information about data protection and ethical issues. In order to achieve a professional level of personal data management a template will be distributed to all data collecting partners. As not only within the pilots personal data might be collected, all partners have to check their research for collected personal data. The template includes the following questions which all investigators have to fill in concerning private information:

#### What kind of data will be recorded, stored and why?

It has to be clear to the supervisor which kind of data will be stored e.g.:

Following the UCD approach as outlined in A1.1.4, following phases are to be foreseen for the pilots:

- Cognitive walkthrough (early stage, use system specifications, scenario-based role play, qualitative data);
- Feature inspection (early stage, use scenario-based end results to be obtained from the use of the product, qualitative data);
- Think aloud (vocalise thoughts, feelings and opinions whilst performing tasks, qualitative data);
- Co-discovery method (observe a pair of participants performing tasks together, workplace applications);
- Question asking protocol (prompt the participants by asking direct questions);
- Performance measurement (time, error rate, quantitative data);
- Wizard of Oz (use mock-ups from low-fidelity to high-fidelity);
- Questionnaire (qualitative and quantitative data).

- Will the data be transferred?
- Data ownership?
- Is the data connected to other information?
- Will the data possibly commercially exploited?
- Length of storage?
- Where data will be stored, - according to which national legislation?
- Who will access the data?
- Who will supervise the data protection?

## 9 General Legal Framework for the respective European Countries: Relevant Local Ethics Research Committees

The following paragraphs give an overview about the general legal framework and concepts of the Ethics Code of Conduct for VERITAS. After this, in the second part of the chapter, LREC will be introduced.

Data collection especially with people who need special assistance or more time for distinct purposes gives rise to a host of legal and privacy issues. Privacy and legal issues are presented under the headings of legitimacy issues, and legal issues. The first group includes a cluster of issues related to the question: ‘why we do we need VERITAS and should we perform VERITAS?’, while the second group hints at the limits that the rule(s) of EU law puts on the data collection and management.

### 9.1 Legitimacy issues of VERITAS

*Freedom and personal responsibility:* The use of Virtual Reality (VR) for designing rises some classical ethical questions (e.g.: Why shall VERITAS/VR be used? Can it be trusted in terms of personal freedom, mental integrity? To one approach no private authority or government body has the status or right to enforce anyone to use VERITAS system (e.g. in the industry a boss could force an employee to use the VERITAS system for designing) but as an end- user nobody can be forced e.g. to take part in the pilot studies. As a consequence it is left to the individual (to some extend more to the disabled end-user than the designer) to use or interact with VERITAS voluntarily (within the framework of the current law).

*Role of private parties and accountability:* Private parties most likely have the same level of interest in implementing VERITAS than government officials. Private parties “the industry” can use the VERITAS VR tools in order to successfully create products for a big and growing market (people with special needs) and the government officials have the duty to provide such technologies in order to support “access for all” (e.g. E-inclusion initiative; [http://ec.europa.eu/information\\_society/activities/einclusion/index\\_en.htm](http://ec.europa.eu/information_society/activities/einclusion/index_en.htm)). Private as well as government actors will not only be in charge of incorporating legal norms in technologies, but also of enforcing, supervising, and correcting wrong norms incorporated in technologies (for instance discriminatory practices with respect to the “access for all” approach).

*Human rights:* Human rights, as part of public law, do not contemplate consent or choice. To express their meaning, in the context of product development (VERITAS tools and platform), human rights have to be considered ahead of the implementation, or integrated in the design of the technologies. Therefore the Ethics Advisory board will meet regularly.

*Privacy.* For privacy issues protection please see chapter 5 in the Ethics Manual!

With regard to the pilots in VERITAS, the authors would like to raise the attention to "Privacy in the workplace". As VERITAS is developed and partly tested in working environments it should be brought in mind that 'Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. [...] It is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not'. (ECHR, Niemitz v. Germany, 23 November 1992, Series A nr. 251/B, par. 29). Therefore personal opinions at the workplace for the developed tools have to be respected in the same manner as if they were given outside the job.

In the following, the principles of data protection legislation are recalled and enhanced.

*Proportionality and purpose limitation (1):* In the field of VERITAS, it is not easy to elaborate the principles of proportionality and purpose limitation. Previously collected data may serve for later developed applications or discovered purposes, for which all legal requirements must be fulfilled.

*Proportionality and purpose limitation (2):* In the field of VERITAS, the proportionality and purpose limitation principle entail that it is not necessary - for the purpose of design guidelines and - to store especially any medical data in central databases with link to the owner, but in an anonymous way and access shall remain also in the control of the user (via anonymisation list, see Article 29 Data Protection Working Party, Working document adopted on 1 August 2003, par. 3.2). Meaning, if a user wishes, that his or her data will be destroyed or removed from any kind of server, this shall be done.

## 9.2 Legal issues

*National and EU level:* It must be pointed out that concrete legal requirements on the data collection depend also on national legislation.

*Location data:* Directive 2002/59/EC introduces 'location data' as a type of data to be specially protected. Up to now, no monitoring (e. g. GPS) data are included

*Health data:* The project foresees data gathered through technologies such as EEG, ECG as well as the measurement of other medical parameters through respective technologies. These are sensitive data which must be protected against purposes other than the declared once (function creep), e.g., for medical diagnosis, vigilance analysis of Co-workers and employees, employment conditions or insurance. Disclosure of health data also raises serious privacy concerns.

*Employer - employee power dynamics:* (data processed in working environments) Access to the data? Only the employee? Also the employer? Will the data be kept for other purposes that ensuring the security of the security infrastructures? Which security measures are required during the collection, communication and eventual storage of the data? Are location data and sensitive data specially protected? Is there any special approach to identity management to be promoted in these situations? For identity management and data protection please be referred to chapter 4 of the Ethics Manual.

*User control and user empowerment:* User control and user empowerment should be taken into account during the design of the technologies and also during the design of the information systems to implement the technologies. Therefore End User Organizations are “on board” at an early stage of the development cycle.

*Data Retention Directive:* Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (the Data Retention Directive) does not apply to the domain area of VERITAS. However the Directive exposes the possibility of large scale data collection without specific purpose limitation. Only anonymised data will be collected.

### 9.3 Medical data is personal data

While discussing the interpretation of ‘any information’ contained in the Directive (95/46/EC), the Article 29 Data Protection Working Party opinion on the notion of personal data (‘/2007, adopted on 20 June 2007) makes ‘special reference’ to medical and biometric data. These data are defined as ‘biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability’. The Article 29 WP’s opinion supports the idea that biomedical templates are to be considered personal: ‘A particularity of biometric data is that they can be considered both as *content* of the information about a particular individual as well as an element to establish a *link* between one piece of information and the individual (this ECG etc. belong to a specific, identifiable person. As such, they can work as “identifiers”. In its opinion, the Article 29 WP makes no distinction between ‘soft’, ‘robust’ ‘special’, ‘behavioral’, ‘activity related’, ‘physiological’ et cetera biometric and medical data.

### 9.4 Relevant provisions of the Data Protection Directive

Principles relating to data quality (Art. 6): Biomedical information and personal opinion must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Art.6.1b); The collection and processing must be adequate, relevant and not excessive in relation to the declared purposes (Art. 6.1c);

The responsible entity is the data controller (Art. 6.2 - 16, 17, 18, 19): There has to be a responsible controller to ensure data protection rights and duties. For the purpose of article 6.1, the responsible entity is the data controller (6.2);

Criteria for making data processing legitimate (Art. 7): No data collection can go unnoticed of the subject that is being monitored. The goal is that the individual is aware of all types of data about him/her that are collected;

The processing of special categories of data (Art. 8): Medical data should be collected and processed fairly and lawfully; the processing of medical data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade - union membership and the processing of data concerning health of sex life should be prohibited as a rule;

Information in cases of collection of data from the data subject (Art. 10 - 11): The data subject has a right to know about the processing and the use of the processed biometrics;

Exemption and restrictions (Art. 13): The principle is that all data subjects are endowed with a right of access to their data and to obtain rectification, erasure or blocking of data when the processing violates the provisions (e.g. incomplete or inaccurate nature of the data). In some cases, however, these rights are restricted to safeguard national security, defence, public security, prevention and criminal investigation, economic or financial interests of states, rights and freedoms of others;

Automated individual decisions (Art. 15): Every data subject has a right not to be subject to a decision which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc;

Security of processing and contents of notification (Art. 17 and Art. 19): Especially personal medical data may not be disclosed to third persons if this doesn't follow from the declared purpose;

Obligation to notify the supervisory authority (Art.18): Before processing any medical information the supervisory body has to be notified of the purposes of the processing;

#### *Other relevant documents*

Art.29 Working Party "Opinion 3/998 on Public sector information and the protection of personal data; Contribution to the consultation initiated by the European Commission in its Green Paper entitled "Public sector information: a key resource for Europe" COM (1998) 585 Stating that *"The computerization of data and the possibility of carrying out full - text searches create an unlimited number of ways of querying and sorting information, with Internet dissemination increasing the risk of collection for improper purposes. Furthermore, computerization has made it much easier to combine publicly available data from different sources, so that a profile of the situation or behavior of individuals can be obtained. In addition, particular attention should be paid to the fact that*

*making personal data available to the public serves to fuel the new techniques of data warehousing and data mining. Using these techniques, data can be collected without any advance specification of the purpose, and it is only at the stage of actual usage that the various purposes are defined. So, all of the technological possibilities with regard to data usage need to be considered”.*

## 9.5 Privacy Guidance in Technology Design

As all computerized systems, also VERITAS implies some privacy and data protection risks, which are, however, mitigated by two major facts. First VERITAS system does not store raw medical samples. They are immediately converted into digital files and the raw samples are erased. All that remains are ‘templates’, which are of no use outside of the system, and cannot be reverse engineered to recreate the raw sample. Second VERIATS applications are not expected to be ever used for identification purposes, and consequently they will not use large reference databases. VERITAS privacy issues include,

1. Transparency
2. Consent
3. Proportionality, Limitation
4. Extraction and use of additional information in biometric reference data
5. Security and Identity Theft

## 9.6 Transparency

The most fundamental principle of any data collection system is the Principle of Transparency. In the EU no single data collection can go unnoticed of the subject that is being monitored (that is, as long as the subject can be personally identified). VERIATS is not suited for covert operation, because subjects must confirm their participation.

It would be helpful to provide the data subject with a notice, which reminds the person that he/she is in a continuously monitored environment. Depending on the application domain, different notification mechanisms could be implemented. The goal is to make the person aware that personal, sensitive, data are collected.

## 9.7 Consent

EU Directive prohibits any collection and usage of personal information, except for certain legal procedures (law enforcement, public health, etc) or when explicitly consented by the individual. The most common form of explicit consent is still the written contract. By showing the signature of the data subject under a corresponding piece of text, collectors can in most cases effectively demonstrate that they have received the explicit consent of the subject. In the VERITAS context, however, explicit and informed consent is not that easy to come by. The critical point is whether the subject merged into a seamless, invisible, and continuous monitoring of his/her actions and behaviour might ever have a true understanding of what it means in terms of privacy breach. With several sensors collecting information it is hardly thinkable that a person can

really realize the number of personal details that could be collected on him/ her. In such a context it is advisable that the investigator let the participant repeat the basic of the study in his/her own words.

Informed consent form should cover:

1. a clear definition of the purpose for which personal and medical data are going to be used
2. a clear definition of what data, if any, could be ever legitimately obtained by law enforcement agencies because of security / forensic reasons
3. a clear and easy understandable definition of what medical conditions could be detected by the system
4. declaration that the system is not for medical detection, but whether any incidental medical findings happen, the subject will be informed and advised to contact a MD
5. whether any personal data is stored and, in case, what data, for what length of time, when it is erased, who is the data controller
6. declaration that no personal data will be ever transferred out of the system
7. declaration that no data will be ever commercialized or, for any reason, given to a third commercial party
8. declaration that no data will be ever used for discriminating against any subject in the working place
9. declaration that no additional, ancillary, information, which is not relevant to VERITAS, will be ever stored or used

## 9.8 Proportionality, Limitation

The principles of Proportionality, Minimization (only data strictly necessary for the purposes of the system must be collected), and Use Limitation are the other pillars of a fair information policy. In essence, they require that

- data must be collected only for a well- defined purpose which is proportionate to the

means used (proportionality)

- only data strictly relevant for that purpose can be collected (data minimization)

- data can be kept and used only as long, and as far, as it is necessary for the purpose (limitation)

Together with pseudonymization (see below), these principles might save both time and effort that would otherwise be spent in order to properly collect, protect, and manage large amounts of sensitive personal information.

## 9.9 Security and Identity Theft

When talking about security, three areas are typically addressed:

- (1) Confidentiality;
- (2) Integrity;
- (3) Accessibility.

Confidentiality has been defined by the International Standards Organization as, "ensuring that information is accessible only to those authorized to have access." Confidentiality limits data to specific users based on needs and

restricts access to everyone else. Confidentiality tools include file access permissions, network access control lists, and firewall rule sets. According to Wikipedia, Integrity "*means ensuring data is "whole" or complete, the condition in which data are identically maintained during any operation (such as transfer, storage or retrieval), the preservation of data for their intended use, or, relative to specified operations, the a priori expectation of data quality.*"

It is advisable that some protections are implemented from the design phase, they could include that

- 1) personal data should not be stored together with reference data.
- 2) apart from sensors no other components or interfaces of VERITAS system should be accessible to users.
- 3) Reference data can be stored fragmented and different encryption keys could be used for these fragments.
- 4) All data should be pseudonymised. A pseudonymous identifier is an identifier that cannot, in the normal course of events, be associated with a particular individual. Pseudonymity does not provide true unlinkability, but the link is known only to system operators and it is not publicly disclosed.

Other possible security measures include:

1. Protective measures against infiltration with unauthorized reference data;
2. Detection measures for copies of personal data;
3. Physical protection of core parts of the systems and access control measures;
4. Logging of transactions and appropriate auditing of the systems.

## **9.10 Summary (VERITAS Ethics Rules)**

### **Transparency**

1. Implement a system notification mechanism that makes the subject aware that he is merged into a sensor network and that his performance is continuously monitored
2. Subjects should be explicitly notified when sounds are recorded.
3. Some other regular notice – be on the PC screen or other – should remind the subject that he is continuously monitored.
4. No recorded video or audio will be permanently stored in the system. They will be initially recorded on a computer hard disk, and erased as soon as they are no longer necessary
5. Video, audio, and other data captured will not be used for any other different purpose.
6. Recorded material will never be sold or given to any third party for any reason, be scientific or commercial.

7. Should any medical information be disclosed, it will remain strictly confidential and will not be communicated to any third party, employers or supervising authorities included.
8. Should any incidental medical findings arrive; the subject will be immediately informed about it and advised to refer to his GP.

### **Consent**

1. Provide a written consent form before subjects perform the study

#### **Cave:**

During the data collection activities medical information might be disclosed. IT IS THEN IMPORTANT THAT

- 1) the subject is informed about the risk that the VERITAS system can disclose details about his medical conditions;
- 2) the subject is aware that incidental medical findings can theoretically arrive. In case of this event, the subject must be preventively informed about the policy followed by the system controllers (e.g., the subject will be referred to the GP, will be referred to another MD, will be advised to contact an MD, etc);
- 3) it is declared that no medical information about the subject will be disclosed to the employer, or to any other third party, except in those cases in which it is legally mandatory (if any).

### **Proportionality, Limitation**

1. Minimize data collection. No redundant data.
2. Never store raw data (possible exception during pilots for testing the system)

### **Security and Identity Theft**

1. No personal data should not be stored together with the reference data.
2. Apart from sensors no other components or interfaces of the biometric system should be accessible to users
3. Reference data can be stored fragmented and different encryption keys could be used for these fragments.
4. All data should be pseudoanonymised (=coded)
5. Protective measures against infiltration with unauthorized reference data should be

6. provided
7. Detection measures for copies of biometric characteristics should be provided
8. Physical protection of core parts of the systems and access control measures should be provided
9. Logging of transactions and appropriate auditing of the systems should be provided

## 10 LREC: Local Research Ethics Committees

The following paragraphs give an overview about the different legal framework in the EU countries which perform any kind of data acquisition within VERITAS. A detailed report about the special characteristics of the situation of the RECs is presented for each country. The description of the characteristics differs between each country which is due to the lack of information taken from the book "Research Ethics Committees, Data protection and Medical Research in European Countries D. Beyleveld (2005)".

### 10.1 UK

#### **Research Ethics Committee for UNEW:**

Newcastle and North Tyneside Research Ethics Committee 2

#### **Chair (currently)**

Professor Philip Preshaw

#### **Coordinator (currently)**

Gillian Mayer; Room 002; TEDCO Business Centre; Rolling Mill Road; Jarrow  
Postcode: NE32 3DT; England

#### **Appointing Authority:**

North East SHA

#### **Regional Manager**

Ann Tunley

#### **Committee Flags**

- Phase 1 Studies in Patients
- Research Involving Adults Lacking Capacity

#### *Relevant legislation*

- 1) Data Protection Act 1998
- 2) Freedom of Information Act 2000 in England, Wales and Northern Ireland
- 3) Environmental Information Regulations 2004 in England, Wales and Northern Ireland
- 4) Privacy and Electronic Communications Regulations 2003

#### *Relevant regulatory authorities and ethical committees include:*

1. Information Commissioner's Office (ICO) <http://www.ico.gov.uk/>
2. ICO documents relevant to VERITAS include:
3. Transferring personal information outside the EEA
4. Good Practice Note - Disclosing information about tenants, 16.11.2005

5. Subject access involving other people's information, 12.07.2006
6. Subject access to health records, November 2001
7. Good Practice Note - Subject access and employment references, 16.11.2005
8. CCTV Data Protection Codes of Practice
9. CCTV systems and the Data Protection Act - when the Act applies
10. CCTV small-user checklist
11. Privacy Enhancing Technologies

### **The Establishment and Regulation of Ethical Review of Medical Research in the UK**

Two kinds of NHSs (National Health Service) RECs were known in the UK until 2004. These two NHS RECs were the local research ethics committees (LRECs) and the multi-centre research ethics committees (MRECs) which were responsible for every research situated in multiple locations. For single-sited research carried out, both of these two RECs could be asked for permission. These two NHS RECs still exist, even a new system has been established.

### **RECs and Clinical Ethics**

In the UK, 63 separate clinical ethics committees (CECs), situated in individual institutions and normally formed on the initiative of interested parties, give clinical ethics advice instead of RECs. These CECs have no formal guidelines pretending membership obligations or actions.

### **The Criteria for REC Review**

Required by the Department of Health, every research involving patients, user service, has to guarantee it meets ethical standards.

### **Accountability of RECs**

Since March 2004 the COREC is responsible for the health authorities concerning the operational procedures for all RECs and relevant RECs, under the CT regulations, are subordinated to the direct authority of the United Kingdom Ethics Committees Authority (UKECA). A clinical trial research using medicines in humans can only go ahead with their study if the UKECA gives their approval. The ruling officials for UKECA are the Secretary of State Health, the National Assembly of Wales, the Scottish Ministers and the Department for Health, Social Services and Public Safety for Northern Ireland.

UKECA is accountable for ascertaining, acclaiming and observing all RECs which are part in the review of clinical trials at the time when CT regulations came into effect. UKEC is able to decide what kind of research project a REC has to review or the section in which it will work and if used to the UKECA can also eradicate a committee. If necessary the UKECA can also give advice and assistance to a REC.

### **General Powers of RECs**

#### *Approval*

An acclamation of a REC, which can acclaim or refuse a request, is essential for a research to be continued but it is not enough. Supplementary regulatory acclamations are used for certain categories of research.

### *Penalties for Non-Compliance*

RECs are not able to penalize, they can just give reports to the institutions or adequate regulatory bodies and listing all the pertinent points. As a consequence the responsible regulatory body may discipline investigators or other involved persons. Depending on the severity of this offence, the consequence for an individual distorting the data could be an imprisonment. The penalties will not be implemented by the RECs but through the licensing authority.

### **General Legal Responsibility of RECs**

In the case of a suspected breach of the law, RECs have to notify the researcher and the responsible authority about their worries whereupon the researcher and the authority should search for legal counsel.

### **Practice of RECs**

If the REC is confronted with an unlawful but ethical request, it may accept the application by informing the investigators about the legal situation and consequences. It is not the REC's responsibility to interpret the law. The responsibility of a REC ends with informing the researcher or appropriate sponsors about legal misgivings of the study. Additionally it is the researcher's or sponsor's responsibility to search for legal advice,

#### 10.1.1 Summary of UK RECs

Type of REC	LRECs	MRECs	RECs of particular Organisations
Where situated?	NHS	NHS	<ul style="list-style-type: none"> <li>○ Medical Research Council</li> <li>○ UK Universities</li> <li>○ Pharmaceutical industry</li> </ul>
Who applies to them?	Researchers	Researchers	Researchers from the institute where the committee is situated
Formal/Informal	Formal	Formal	Informal
National/Regional	Local	Regional	Local
Laws Involved (see below)	Health Service Regulations 2002 Adults with Incapacity Regulations 2002 (Scotland) Medicines for Human Use (Clinical Trials) Regulations 2004	Health Service Regulations 2002 Adults with Incapacity Regulations 2002 (Scotland) Medicines for Human Use (Clinical Trials) Regulations 2004	-
Guidance Involved	Governance Arrangements for	Governance Arrangements for	-

	NHS Research Ethics Committees Research Governance Framework for Health and Social Care Standing Operating Procedures for Research Ethics Committees	NHS Research Ethics Committees Research Governance Framework for Health and Social Care Standing Operating Procedures for Research Ethics Committees	
Membership requirements	Except in Scotland: <18 Members of which one third must be lay members with the remainder being expert members. In Scotland: <18 Members including doctors, a nurse, a pharmacist, a clinical pharmacologist, a person with experience in the treatment of adults with incapacity & 3 lay members.	Except in Scotland: <18 Members of which one third must be lay members with the remainder being expert members. In Scotland: <18 Members including doctors, a nurse, a pharmacist, a clinical pharmacologist, a person with experience in the treatment of adults with incapacity & 3 lay members.	-
Responsible/accountable to whom?	To the UKECA or the body they have nominated e.g. COREC in England	To the UKECA or the body they have nominated e.g. COREC in England	-
Approval or Advisory powers	Approval	Approval	

**Table 5 Summary of UK RECs.**

**Dataprotection UK:**

*Mr Christopher Graham*

*Information Commissioner*

*The Office of the Information Commissioner Executive Department*

*Water Lane, Wycliffe House*

*UK - WILMSLOW - CHESHIRE SK9 5AF*

**Tel.** +44 1 625 54 57 00 (switchboard)

The UK's Data Protection Act has six parts.

In Section I Personal data is described as “data which relate to a living individual who can be identified...

- a) Directly from those data or
- b) Indirectly from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intention of the data controller or any other person in respect of the individual.”

That means that data are personal if the data controller can indirectly identify the data subject. “Personal data includes also information extracted from personal data”. In UK law the anonymization is not covered by the Data Protection Act.

## 10.2 France

Comité Consultatif National d'Ethique (CCNE)

35, rue Saint-Dominique 75700 Paris

FRANCE

Phone : 33 01 42 75 66 42

Fax : 33 01 42 75 66 49

The CCNE is a strictly consultative body. It acts when questions are “referred” to them, dealing with societal issues related to the progress in knowledge in the field of health and life sciences.

### **The role of Ethics Committees in Relation to French Biomedical Research: Protection of the person and personal data**

#### **The Establishment of Committees**

Before starting a clinical trial, an approval of an ethics committee is required (European Directive of 4 April 2001). The committee has to make sure that the project fulfills ethical standards for research and that the protection of every participating person is guaranteed. For every clinical trial the subjects consent is needed. In France there is a differentiation between committees which are used to give a verdict on ethical issues and committees which responsible for the human rights to be respected.

The law of 9 August 2004 assures the protection of the participating persons rather than the processing of their personal data. The CNIL (Commission Nationale de l'Informatique et des Libertés) has the function of supervising the use of personal data. The CNIL has 15 members mandated for five years of which 12 are appointed by their peers: two deputies, two senators, two members of the Economic and Social Committee, two members of the Cour de Cassation, the Council of State and of the Court of Auditors, qualified persons (three because of their knowledge of computer science applications or issues relating to personal freedoms and two because of their knowledge of data processing techniques and who are selected by the president). The president is chosen by the members of the CNIL. The CNIL has two month, with the option of an elongation, to provide announcement of its decision. This announcement is not of an ethical nature but of a legal one.

The committees have a time-limit of five weeks, after the submission of the research protocol by the investigator, to present a “reasoned opinion on the condition of validity of the research with regards to the protection of persons”. Depending on these opinion the written information has to be suitable,

intelligible and exhaustive and it has also to be ensured that the way of achieving the subjects consent is clear and that the subject had enough 'thinking time' and that he /she has the right to give a prohibition. The opinion of the committee is essential but not sufficient. The authorization from the competent authority is also needed. For research focusing on drugs, contraceptives or progesterone-inhibiting product the French Agency for the "Sanitary Security of Health Product (AFSSAPS)" is responsible, for every other research the competent authority is the Minister of Health. These Committees have to be independent.

The National Consultative Committee for the Processing of Information in the Health Sector has 14 members and one president. All members are scientists, which are mandated for three years with the possibility of one renewal. The committee has to follow the joint agreement between the Minister for Health and the Minister for Research.

### **Powers of the Committees**

Committees have to guarantee the protection of the participants and the legal processing of their data. Before starting a research study on humans, the consultation of a Committee for the Protection of Persons is needed and then to get authorization from the AFSSAPS or the Ministry of Health. The punishment for not consulting these committees and authorities is 15000 Euros. For processing the data the authorization from the CNIL is needed. Only the CNIL is entitled to authorize the use of processing data for the purpose of research in the health sector.

The major aim of all the different committees is to assure the legal compliance of the research project partners. An unlawful project cannot be accepted even it were in public interest. The CNIL gives his authorization only if the conditions of the law were followed and the consent of the data subject is lawful. Data enabling the identification of the persons concerned has to be encoded prior to their transmission. The direct or indirect identification of the data subject through the presented results of the data processing operation shall be forbidden.

### **Recourse against the Committees' Decisions**

The committees' opinion cannot be appealed for annulations of administrative acts, since this is limited to Acts considered to be 'holding a grievance'. "If a committee makes a mistake in the execution of its remit, the state assumes responsibility."

Only the CNIL, as an independent administrative authority, has the power to authorize projects. The CNILs decision can" constitute a grievance and be considered as an act that can be appealed to the administrative judge".

#### **10.2.1 Summary of French RECs**

<b>Type of REC</b>	Committees for the Protection of Persons (CPPs)	National Consultative Committee on the processing of Information in the Health	CNIL-Data Protection Supervisory Authority
--------------------	---	--	--

		Sector	
<b>Where situated?</b>	48 CPPs in the French regions		Paris
<b>Who applies to them?</b>	The sponsor	The Controller	The Controller
<b>Formal/Informal</b>	Formal	Formal	Formal
<b>National/Regional</b>	Regional	National	National
<b>Laws Involved</b>	Law Hurriet-Serusclat of 20th December 1988, amended by the Law of 9th August 2004	Law of the 1st July 1994 modifying the 1978 Act: Official Journal 2nd July 1994 Decree No. 95-682 of the 9th May 1995 for the application of Chapter V of the 1978 Act	Law of the 6th January 1978 on data protection. Law of 1st July 1994 modifying the 1978 act.
<b>Guidance Involved</b>			Recommendation of the 4th February 1997 of the CNIL on the processing of health personal data
<b>Membership requirements</b>	12 members per CPP: General practitioners Specialist doctors Pharmacists Nurses Psychologists An ethicist A sociologist a lawyer Representatives of patients' associations	14 members and 1 president nominated for 3 years. All members are scientists.	17 members nominated for 5 years: 2 Deputies 2 Senators 2 Members of the Economics and Social Committee 2 Members or Former Members of the Cour de Cassation, of the States Council and of the Cour des Comptes 2 Qualified persons in Computer Science 3 Persons Designated by the Council of Ministers 1 President elected by the CNIL's Members
<b>Responsible/accounta</b>	Totally	Subordinate to	Independent

<b>ble to whom?</b>	independent	the Ministry of Health	Administrative Authority. Its decision can be appealed to the Administrative judge
<b>Mission</b>	<p>Remit includes any trials or experimentation on humans for the purpose of developing biological and medical knowledge, either for a therapeutic or non-therapeutic purpose.</p> <p>Providing an opinion on whether the rules on the protection of the person involved in the research have been respected or not in each submitted research protocol. Consent is especially considered.</p> <p>Do not provide ethical opinions.</p> <p>Do not have a legal role in relation to the protection of personal data but in practice can be consulted on this topic</p>	<p>Competent only for the processing of personal data in health matters.</p> <p>Give an opinion on the methods of the research in relation to the data protection law.</p>	Supervision, information and advice in relation to the data protection law.
<b>Approval or advisory powers</b>	Advisory powers. It is however compulsory to receive their opinion in order to obtain authorisation from the French Agency for the Sanitary Security of Health	Approval powers	Approval powers: The CNIL gives its authorisation.

	Products or from the Minister for Health.		
<b>Type of REC</b>	National Consultative Ethics Committee	Ethics Committees linked to research organisations	Local Ethics Committees
<b>Where situated?</b>	Paris	Scientific organisations eg: INSERM and CNRS	hospitals
<b>Who applies to them?</b>	Presidents of Parliamentary Assembly, Members of the Government, Foundation of Public Usefulness, Public Organisation of Research.	CNRS: Administrative Council of the CNRS, or the Scientific Council of the CNRS or the General Director of the CNRS or the Ethics Committee itself	
<b>Formal/Informal</b>	Formal	CNRS: Formal	Informal
<b>National/Regional</b>	National	In research organisations	Local
<b>Laws Involved (see below)</b>	Decree No. 83-42 of 23rd February 1983 Amendments to the Law Hurriet-Serusclat of 20th December 1988 by the Law of 9th August 2004	CNRS: Decree no. 2000-1059 of 25 October 2000, Article 21-2	
<b>Guidance Involved</b>		CNRS Charter	
<b>Membership requirements</b>	39 members and 1 president: 5 persons belonging to the 'main philosophical and spiritual family' chosen by the President of the Republic. 19 persons chosen for 'their competency and interest in ethical issues'	CNRS: 1 President chosen for 4 years by the General Director of the CNRS on the proposition of the Administrative Council. 12 members, scientists or persons	

	15 persons belonging to the research sector	coming from the civil society.	
<b>Responsible/accountable to whom?</b>	Independent	CNRS: Independent ethics committee near the Administrative Council of the CNRS.	
<b>Mission</b>	Reflection on ethical and social issues in biological, medical and health sector. Give general opinion on general cases- never on individual cases. Do not review research protocols.	General mission to consider ethical issues Maintain dialogue between the biomedical research community and society. Do not review research protocol.	Give opinions especially on clinical ethics issues met in practice.
<b>Approval or Advisory powers</b>	Advisory powers. No legal effects.	Advisory	Advisory powers. No legal value

Table 6 Summary of France RECs.

**Dataprotection France***Commission Nationale de l'Informatique et des Libertés*

8, rue Vivienne, CS 30223

F-75002 Paris, CEDEX 02

**Tel.** +33 (0) 1 53 73 22 22**Fax** +33 (0) 1 53 73 22 00**Laws**

- Law no. 2004-801 of 6 August 2004 modifying the law Huriet-Sérusclat (in French).
- Decision for the creation of the Ethics Committee of the CNRS: Decision of the 20th August 2002 (in French).
- Code of the Public Health (in French)
- Ethics Committee of the CNRS: Decree n°2000-1059 of 25 October 2000.
- Law No 94-548 of the 1st July 1994 on the processing of personal data for purpose of research in the health sector (in French).
- Law Huriet-Sérusclat No 88-1138 of the 20th December 1988 on the protection of persons participating in Biomedical Research (in French.)
- Law No 78-17 of the 6th January 1978 on Informatics and Freedoms (in French).
- Legifrance - contains French legislation, codes and laws in preparation
- Organisations and Ethics Committees

- National Consultative Ethics Committee
- List of the CCPPRBs -former CPP system before 2004 Law
- CNIL
- CNRS - COPE
- INSERM (in French & English)

In French law the definition of personal data is written in Article 2 of the Directive: "Personal data is any information related to an individual identified or who can be identified, directly or indirectly by reference to an identification number or to one or more factors".

Anonymized can be seen as the antonym of identified, what means that anonymized data cannot be directly or indirectly linked to the individual anymore.

The Data subject has to give a written consent. Article 7 of the law says about this consent: "...processing of personal data must either have received the consent of the data subject, or be necessary to satisfy one of the conditions..."

The data subject has the right to request the data controller get:

1. "confirmation that his or her data has been processed,
2. Information on the purpose of the processing and the recipients of the data and,
3. The disclosure of these data in an accessible form. This refers to the methods of the Civil Law as modified by the new Law (Article 39)."

Under certain conditions the transfer of data to third countries is possible with a sufficient level of protection.

### 10.3 Germany

German Ethics Council

Berlin-Brandenburgische Akademie der Wissenschaften

Jaegerstr. 22/23

D-10117 Berlin

E-Mail: kontakt@ethikrat.org

Head of office

Dr. Joachim Vetter

#### *Relevant legislation*

- Act on the Establishment of the German Ethics Council of 16 July 2007 (Federal Law Gazette I p. 1385), entered into force on 1 August 2007
- Federal law on data protection (Bundesdatenschutzgesetz)

#### **The RECs in Germany**

In Germany 52 civic, law-based RECs were set up in consistence with the state law. These committees control the moral integrity of research on human subjects.

#### **The Composition of RECs**

In Germany, significant variations concerning the number and profession of the members of different RECs exist. Most RECs have between 5 and 19 members; which can range from four, up to one REC with 32 members. The majority of RECs are made up of medical practitioners with the involvement of a lawyer, philosophers and theologians. Biometricians are represented in barely a third of RECs, which is surprising in view of the necessary and difficult calculations for

testing the scientific content of the design. Only in some cases patient representatives or those who care for patients are included in an REC consultation, which should be changed in order to better integrate end-users/patients concerns. For VERITAS it should be discussed, if end-user should be included in the Ethics Advisory board.

### **Diversity in Fees Charged**

The fees for the REC's differ between 400 and 2700 Euros; sometimes for a second evaluation, the RECs frequently claim fees. Pharmaceutical firms who only want to do a clinical trial sometimes have to spend around 25000 and 50000 Euros for the fees.

Generally, members work in an honorary capacity, which means their work for the REC is not a source of income and some RECs pay their members an 'attendance allowance'. Financial compensation is frequently paid by RECs to any expert consulted in the course of an REC procedure.

### **The Workload of RECs**

The RECs have to deal with 19 to 600 applications, on average 244, per year. In addition every commission gets around 100 protocol modifications.

### **Historical Development of RECs**

The first time REC appeared as an obligatory element in research was in 1972 when a new medical research program has been set up in Germany. In 1975, The Declaration of Helsinki has been rewritten by the World Medical Association which was a significant event for the growth of RECs in Germany. After the revising, an independent body has to be consulted before the conduction of research involving human subjects. Therefore the REC became an element of the normative force on medical ethics regulating medical research.

In the following, RECs were neither under explicit legal nor public scrutiny. The REC was not based on the law governing the medical profession but based on private law. REC became more and more important in pharmaceutical industry's clinical drug trials and some medical research institutes set up their own, private RECs. Primary in 1985, RECs received explicit legal recognition in medical professional law, in 1988 the obligation was made more compulsory and in nowadays RECs are a regular element of the official Model Professional Code for Medical Practitioners.

### **RECs and Clinical Ethics Committees**

In 2003 67 hospitals, of which 51 are confessionnal, had ethic consultation in form of clinical ethics committees. RECs and clinical ethic committees have been instigated as two functionally distinct advisory bodies. An important aim of establishing clinical ethics committees was to strengthen the profile of the religious and moral values of the hospitals.

### **The Complex Legal Status of RECs in Germany**

A common legal regulation is still missing for the RECs in medical research; uniformed appreciation of RECs have only achieved in the special statutes of the Medicinal Product Act, the Law on the Trade in Drugs and in the law regulating medical trials with radioactive material and protection against

radiation. RECs reviews were also initiated in the law regulating the medical profession, in the medical professional codes at the state level and in some regulations, existing in big research institutes. Because of the incomplete consistent guidelines, problems arose repeatedly in the current practice of medical research.

### **Critique of the Legal Over-Regulation of the Review Process in RECs**

Critics (in particular medical doctors) fear that such guidelines would prompt an extreme legal over-regulation of RECs' monitoring and counseling actions. In the section of medicinal drugs the controlling of legal regulation system has already been established and is formulated in the EU Directive 2001/20/EC "Good Clinical Practice".

### **The Supremacy of Public RECs over Private RECs**

The advices of private RECs have not been completely acclaimed by the professional public law-based RECs; therefore researchers and industrial sponsors are not very interested in asking them for recommendation.

### **Current Problems with the EU Homogenization of RECs**

The European regulations on research with human and animal medicinal drugs and the guidelines for the use of good clinical practice were legally absorbed into German law in 2004, in 12<sup>th</sup> amendment of the Medicinal Drugs Act. It is written that only comprised RECs in agreement with state law, like REC's located in university clinic should be able to estimate clinical trials for medicinal drugs. Multi-centre clinical trials have to present their request to the REC connected with the accountable investigator for the study. This generalized judgment procedure has been criticized by the Working Party of Health Care Ethics Commissions whose opinion is that more than just one nationwide REC is needed to build a rational estimation. Also the National Medical Association, the German Union of National Health General Practitioners and the Medicinal Drugs Commission of the German Medical Profession spoke out a related opinion and additionally they wanted the investigator to be a medical doctor, like it was used to be in the past. Currently the investigator has to be appropriately qualified, what means that he/she is used to have at least two years of experience in clinical trials of medicinal drugs.

#### **10.3.1 Summary of German RECs**

<b>Type of REC</b>	National Ethics Council	Local RECs	Local RECs	'Free' RECs
<b>Where situated?</b>	Berlin-Brandenburg Academy of Sciences	Medical Research Institutes	Medical Faculties	
<b>Who applies to them?</b>	Federal government or the Bundestag can ask them to formulate opinions and they can also set their own	Researchers	Researchers	Researchers

	agenda			
<b>Formal/Informal</b>	Formal	Formal	Formal	Formal
<b>National/Regional</b>	National	Regional	Regional	Regional
<b>Laws Involved (see below)</b>	Established by Federal Decree 2 May, 2001	Medicinal Products Act (MPG) Medicinal Drugs Act (AMG) - amended 2004 Transfusion Act 1998	Medicinal Products Act (MPG) Medicinal Drugs Act (AMG) - amended 2004 Transfusion Act 1998	Medicinal Products Act (MPG)
<b>Guidance Involved</b>	Declaration of Helsinki	Declaration of Helsinki	Declaration of Helsinki	Declaration of Helsinki
<b>Membership requirements</b>	25 members - consisting of prominent representatives from science, medicine, theology, philosophy, sociology, law, ecology and economy	Majority have 5 -19 members Membership consists of mainly medical practitioners with the involvement of a lawyer	Majority have 5 -19 members Mostly medical practitioners with the involvement of a lawyer	Majority have 5 -19 members Mostly medical practitioners with the involvement of a lawyer
<b>Responsible/accountable to whom?</b>	Federal Chancellor	Institute where situated	State Chambers of Physicians	Institute where situated
<b>Approval or Advisory powers</b>	Advisory	Approval	Approval	

Table 7 Summary of German RECs.

**Dataprotection GERMANY**

*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*

*Husarenstraße 30*

*53117 Bonn*

**Tel.** +49 (0) 228 997799 0 or +49 (0) 228 81995 0

**Fax** +49 (0) 228 997799 550 or +49 (0) 228 81995 550

**e-mail:** [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

In the Federal Data Protection Act (FDPA) personal data is described as “any kind of information about the data subject himself or herself or other circumstances relating to him/her.” The data protection ends in case of death. After anonymization the data are out of scope of the FDPA, so the prospective use of anonymized data for different intentions is possible.

In general, personal data can only be collected or processed if the law offers a provision authorising the use of the data or with the written consent of the data

subject. The FDPA proposes additional justifications (terror attack, etc.). Any given consent must be based on a free decision of the data subject and in written form. Additionally, consents will only be accepted if the data subject effectively knows what he or she consented to. The subject has to be informed and understand the purpose of the collection, processing or use of personal data.

## 10.4 Belgium

### 10.4.1 Summary of Belgian RECs

Type of REC	<u>Consultative Committee for Bioethics</u>	Hospital	Outside hospital
Where situated?	Centrally	Hospital	e.g. faculty of Medicine, pharmaceutical firms, professional associations
Who applies to them?	On own initiative Government Scientific research body Healthcare provider Local REC	o researchers	o researchers
Formal/Informal	Formal	Formal	Formal
National/Regional	National	Local	Local
Laws Involved (see below)	Royal Decree of 27 September 1994 Royal Decree of 22 September 1992	Royal Decree of 27 September 1994  Royal Decree of 22 September 1992	Royal Decree of 27 September 1994  Royal Decree of 22 September 1992
Guidance Involved	-Declaration of Helsinki -EC-GCP Guidelines -ICH-GCP Guidelines -Code of Deontology of the National council of the Order of Doctors	-Declaration of Helsinki -EC-GCP Guidelines -ICH-GCP Guidelines -Code of Deontology of the National council of the Order of Doctors -Consultative Committee on bioethics	-Declaration of Helsinki -EC-GCP Guidelines -ICH-GCP Guidelines -Code of Deontology of the National council of the Order of Doctors -Consultative Committee on bioethics
Membership requirements	35 actual members & the same number	8-15, of both sexes:	8-15, of both sexes

	of substitutes: balance between Christians/Non- Christians, French & Dutch speakers, those with a scientific background & those with a background in philosophy, law & social sciences, and also between male & female.	A majority of doctors connected to the hospital At least 1 GP not connected to the hospital At least 1 nurse connected to the hospital A lawyer <i>Other interested persons,</i> who cannot be: Director of the hospital Head doctor President of the Medical Council Head of Nursing	
<b>Responsible/accountable to whom?</b>	To government	To the medical faculty	To the body responsible for the institute
<b>Approval or Advisory powers</b>	Advisory	Approval	Approval

**Table 8 Summary of Belgian RECs.**

### **Dataprotection Belgium**

*Commission de la protection de la vie privée*

*Rue Haute, 139*

*B - 1000 BRUXELLES*

**Tel.** +32 2 213 8540

**Fax** +32 2 213 8545

**e-mail:** [commission@privacy.fgov.be](mailto:commission@privacy.fgov.be)

### **10.5 Greece**

Hellenic Center for Biomedical Ethics  
G. Gennimata 5, 162 31 Vyronas, Attica  
GREECE

Tel.: +30 210 7648 340

Fax : +30 210 7660 203

E-mail: [info@bioethics.org.gr](mailto:info@bioethics.org.gr)

[bioeth@otenet.gr](mailto:bioeth@otenet.gr)

#### *Relevant legislation*

Law 2472/1997 of the Hellenic Parliament

*Relevant regulatory authorities and ethical committees include:*

1. Hellenic Data Protection Authority <http://www.dpa.gr/>
2. The Hellenic Parliament – Standing Committee for TA [<http://www.parliament.gr/>]
3. The National Bioethics Commission <http://www.bioethics.gr>
4. Decision 63/2004 CCTV cameras on the Attica road network (could be of relevance for the automotive domain)
5. Decision 58/2005 Traffic Management Cameras (could be of relevance for the automotive domain)

### **Establishment of RECs**

The state precludes the intervention in procedures of obtaining and conveying knowledge because of the freedom of research. This right has some limitations justified by the state and additionally other constitutionally protected rights stand above this right.

### **General Powers of RECs**

The acclamation of an REC, who has only a consultant mandate in Greece, is essential for the research. Researchers who do not submit their research for review cannot get acclamation for their work and they cannot publish it, since scientific journals ask for the approval of an ethics committee as a prerequisite for publication.

### **General Legal Responsibility of RECs**

There are no precise legal guidelines about the function of RECs, their terms of reference or question of membership, approach or independence neither through the Greek Medical Association nor through different relevant bodies. RECs are used to perform inside the limits of legitimacy and they are neither allowed to refuse legalized actions, on the basis of the lawful status nor accept illegal ones.

Greece is used to build committees which follow the rules integrated in the Convention, which sets the minimum necessary standard for the defense of the individual, permitting the state to oblige severe domestic rules. Greece has authorized and approved the Convention for the Protection of Human Rights and Dignity of the Human Being concerning application of Biology and Medicine. This Convention requires the member states 'to furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of the Convention'.

Corresponding to the Ministerial Decision, the ethics committees of the Regional Health Councils will give expert opinion and their conclusive choice will be made in including the following points:

- appropriateness of the clinical trial and its design
- risk/benefit analysis
- protocol
- method of selection of participants
- appropriateness of the researcher, the research term and the premises
- researches curriculum vitae

- accuracy and completeness of the written information provided to the participants, the consent procedure and the justification of including individuals who are not capable of consent in the research
- measures in place in case of death or damage caused by the clinical trial
- insurance and compensation covering the researcher's and sponsor's responsibility
- amount and the way of payment of any compensation or indemnity of the researchers and the participants, as well as the content of the contact between researchers and sponsors

Researchers are also obliged to follow the rules of data protection.

### Specific Data Protection Matters

For anonymous information the RECs have to safeguard the parameters 'on the protection of individuals with regard to the processing of personal data'. There is no clear definition about what 'anonymity' denotes. Also the procedure of data anonymization is not explicitly defined. RECs usually accept applications in which data are codified and will be provided anonymously.

#### 10.5.1 Summary of Greek RECs

Type of REC	National Committee of Deontology of Clinical Trials	Regional	Local
Where situated?	National Organisation for Medicines (EOF)	Governing Board of Regional health service	Hospital/Clinic
Who applies to them?	Regional RECs	Researchers, after approval locally	researchers
Formal/Informal	Formal	Formal	Formal
National/Regional	National	Regional	Local
Laws Involved	DYC3/89292 1973/31.12.2003	- A2/oik3061/5.6.1 978 - A6/10983/1/12.1 2/ 1984 -Law 2071/1992 -Law 2519/1997 -Data protection: 2472/1992	- A2/oik3061/5.6. 1978 - A6/10983/1/12. 12/ 1984 Law 2071/1992 Law 2519/1997 Data protection: 2472/1992
Guidance Involved	-Declaration of Helsinki -Oviedo Convention for the protection of human rights & dignity of the human being	-Declaration of Helsinki -Oviedo Convention for the protection of human rights & dignity of the human being	-Declaration of Helsinki -Oviedo Convention for the protection of human rights & dignity of the human being
Membership requirements	6 members, including a lawyer, a theologian, a	-	5 members

	scientist & health science professionals		
<b>Responsible/accountable to whom?</b>	Ministry of Health	-	-
<b>Approval or Advisory powers</b>	Approval	Advisory, although approval is necessary	Advisory, although approval is necessary

**Table 9 Summary of Greek RECs.**

### **Dataprotection Greece**

*Hellenic Data Protection Authority*

*Kifisias Av. 1-3, PC 11523*

*Ampelokipi Athens, Greece*

**Tel.** +30 210 6475 600

**Fax** +30 210 6475 628

**e-mail:** contact@dpa.gr

“Personal data shall mean any information relating to the data subject. Personal data are not considered to be the consolidated data of a statistical nature when data subjects may no longer be identified.” (Article 2)

In Greece the processing of personal data can be performed by the Public or the Private Sector or by natural persons. In the law it is not specified if data protection ends with death.

In Greek Law, the data subjects consent is essential. The subject has to consent the purpose of the processing, the nature of the data and the recipient as well as the name, title and address of the controller or the controller’s representative. The term “anonymization” is not defined in Greek Law, so it is not specified when personal data has to be made anonymous and it does not specify when a person is still identifiable. Article 4 says that “Personal Data, in order to be lawfully processed must be [...] kept in a form which permits identification of data subjects for no longer than the period required, according to the authority, for the purpose for which such data were collected or processed.” The processing of data has to be carried out only by authorized persons (Article 10).

Controllers have to collect personal data fairly and lawfully and only the necessary data are allowed to be processed. They also have to keep data accurate. Controlles have to chose employees “with relevant professional qualifications providing sufficient guarantees in terms of technical expertise and personal integrity to ensure such confidentiality”. (Article 4)

## **10.6Italy**

Comitato Nazionale per la Bioetica

Via della Mercede, 96

00187 Rome

The National Bioethics Committe (NBC) was established by a decree signed by the resident of the Council of Ministers on 28 March 1990 with the task of expressing opinions, and also for the purpose of preparing legislative acts, to address the ethical and legal problems that may arise as a result of the progress in scientific research and technological applications on life. The

Committee formulates opinions and motions, which are published on the website following approval. The NBC establishes and maintains relations at European and International levels.

### **Ethic Committees in Domestic Law**

The ethics committees controlling research are independent, mixed-composition bodies. They are arranged within healthcare units and certified research institutes and controlled by the Ministry of Health.

To get a full picture about research ethics committees, acquisition should be made to the 'National Ethics Committee for Research and Clinical Trials'. The committee is responsible for coordinate ethical and scientific evaluations of multi-centre clinical trials of significant national interest.

### **The Value Conferred on Opinions Rendered by Ethics Committees – Towards 'Professional' Research Ethics Committees**

Beyleveld (2005) criticizes, that the 'ethical committees' often give priority to applications that typically claim technical and professional competence than to discuss ethical and cultural points. The resulting development shows that the ethics committees became 'single multi-functional bodies'.

### **Unresolved Issues A: The (Ir)Responsibility of Ethics Committees**

The first mentionable unresolved issue is the liability which has been refused by the jurisprudence of the ethics committees because of the unsealed nature of their advices. Even the Good Clinical Practice accumulated some doubt about this regulation this issue is still unresolved.

### **Unresolved Issues B: Prerogatives of RECs and Data Protection Laws**

The second unsolved issue is the performance of data protection in regard of the ethics committees. In the Italian legislation data protection is not explicit noted as one of the factors the RECs have to consider for building their opinion. The personal data protection is assumed to the Data Protection Authority.

**Résumé:** Due to the described deficits the EAB will give a special focus on the ethical procedure for the Italian partners.

#### **10.6.1 Summary of Italian RECs**

<b>Type of REC</b>	Local Ethics Committees	Regional Bioethics Committees	National Bioethics Committee	National Ethics Committee for Research and Clinical Trials
<b>Where situated?</b>	Health care facilities & authorised research institutes	all regions	Rome	
<b>Who applies to them?</b>	Researchers	In some cases researchers; mostly advisory to	Parliament, research centres, local ethics committees	

		regional bodies	and individuals	
<b>Formal/Informal</b>	Formal	Formal	Formal	Formal
<b>National/Regional</b>	Regional	Regional	National	National
<b>Laws Involved (see below)</b>	Decree No. 211 of 23 June 2003  Decree 27 April 1992 Decree 15 July 1997 Decree 18 March 1998 Decree 24 June 2003	Constitutional Court Decision 21 December 2000, no.569	Decree 28 March 1990	Legislative Decree no. 502 30 December 1992  Ministerial Decree 23 November 1999
<b>Guidance Involved</b>	Declaration of Helsinki	Declaration of Helsinki	Declaration of Helsinki	Declaration of Helsinki
<b>Membership requirements</b>	2 clinicians 1 expert in bio- statistics 1 pharmacologist 1 pharmacist the medical director or where applicable the scientific director of the Institution 1 legal expert		40 Members designated by Ministers for their biological, legal, scientific or ethic competencies. Within: 4 Members : the Presidents of the National Research Council, the Superior Council for Health, the National Doctors Order, The Superior Institute for Health.	
<b>Responsible/accountable to whom?</b>	Ethics Committees are independent. However the Minister of Health may supervise the mechanisms		Under the supervision of the Prime Minister.	Ministry of Health

	regulating the setting up and functioning of Ethics Committees.			
<b>Approval or Advisory powers</b>	Approval in case of processing of genetic data: An authorisation of the Garante after hearing of the Minister of Health must be obtained.	Approval in some instances e.g.regions where they are the only REC. Advisory: Regional bodies may request their advise.	Consultative Role	Advisory
<b>'Mission'</b>	<ul style="list-style-type: none"> <li>-Approving the performance of drug tests</li> <li>-Assessing biomedical issues</li> <li>Supervising training of health care personnel</li> <li>Assessing medical practice issues.</li> <li>-Ensuring the protection of rights, safety and well-being of any entity involved in testing (Decree 15 July 1997)</li> <li>-Evaluating drugs testing progress reports (Decree 18 March 1998)</li> <li>-Evaluating adverse events and inadequate developments of clinical studies (Decree 18 March 1998)</li> <li>-Monitoring the communication the sponsor is required to provide (Decree 18 March 1998)</li> </ul>	They act as a link & co-ordinating entities between local committees & the National Bioethics Committee	<ul style="list-style-type: none"> <li>- Summarising the programs, aims and results or the research and the experimentation in life science and human health sectors.</li> <li>-Giving opinion and legal solutions to ethical and legal questions resulting from the progresses of research.</li> <li>-Studying the prevention of human and natural area from biological substances and protection of</li> </ul>	They advise the Ministry of Health on ethical & scientific issues. They also co-ordinate the ethical & scientific assessment of multi-centre trials that are of substantial national interest.

			<p>the patients in relation to the new genetic therapies.</p> <p>-Writing codes of conduct to inform the public.</p> <p>-Studying the heredity and the human genome, the procreation, the human rights in biomedicine, protection of persons in final phase, epistemology.</p>	
--	--	--	--	--

**Table 10 Summary of Italian RECs.**

**Dataprotection Italy:**

*Garante per la protezione dei dati personali*

*Piazza di Monte Citorio, 121*

*I - 00186 Roma*

**Tel.** +39 06 69677 1

**Fax** +39 06 69677 785

**e-mail:** garante@garanteprivacy.it

Article 12 of the data protection law says that, if anonymity makes it impossible to pursue scientific research projects, personal data may be used on condition that:

“c. Disclosure of data for the purpose of a defined scientific research project concerning an important public interest has been authorised by the body or bodies designated by domestic law, but only if:

- i. The data subject has not expressly opposed disclosure; and
- ii. Despite reasonable efforts, it would be impracticable to contact the data subject to seek his consent; and
- iii. The interests of the research project justify the authorisation.”

## 10.7 Bulgaria

Bulgaria has two systems for ethical review in medical research:

The **first** is for **clinical trials on human subjects** (not the case in VERITAS). After the approval of the Local Ethics Committee on drugs trials (LEC), for clinical phase I, II or III the trials have to be approved by the Department of Clinical Trials at the Bulgarian Drug Agency (BDA), and then by the Specialized

Committee for Approval of Conducting Clinical Trials (SCACCT) based at the Ministry of Health. For Phase IV trials, the approval is required from the LEC and the BDA. The Ministry of Health defines the membership and operating procedures of the Central Ethics Committee on drugs trials (CEC), which controls the LECs based at regional hospitals. (The LECs are accountable to the CEC, and the CEC to the Ministry of Health.)

The **second** system is the ethical **review of research applications** by the National Science Fund of **local** funding bodies. These are undertaken by local committees at the university or research institute in question, which are controlled by the Central Committee on Research Ethics at the Ministry of Education and Science. These formal committees are regulated by the respective ministries (Ministry of Health and the Ministry of Education and Science).

To our opinion within the scope of VERITAS, the LECs at regional hospitals are of relevance. They are independent bodies responsible for the protection of the rights and safety of participants through reviewing clinical trial protocols, and for the appropriateness of investigators, execution conditions, methods and the materials for obtaining informed consent.

In Bulgaria, the documents required for the review are:

- clinical trial protocol
- the informed consent form
- information on the recruitment procedures
- written information about the participants
- instructions for the investigators
- the clinical card of the participant
- available safety information
- information about reimbursement and compensation of the participants
- details on the insurance of the participants and the investigators
- the investigators' CVs and/or other documents demonstrating their professional qualifications
- other documents deemed necessary"

The central Ethics Committee on Drug Trials has nine members with medical and non-medical education from both genders. At minimum Local committees use to have seven members, of whom at any rate one is from a non-medical profession and one has to be financially and administratively independent from the hospital the clinical trial is carried out.

The assessment of a REC is needed but not sufficient. An application cannot be rejected or approved by the REC whose decision is only a judgment. Other bodies must approve the protocol depending on which of the clinical phases (I – IV). So for the clinical Phase I, II and III the BDA and the SCACCT based on the Ministry of Health have to approve. For Phase IV trials only the approval of the BDA is required. The Good Clinical Practice (GCP) inspectors at the BDA check the study documentation and the compatibility of the protocol with the law on Drugs and Pharmacies in Human Medicine and the relevant regulations.

Nevertheless it is stated in the book “Research Ethics Committees, Data protection and Medical Research in European Countries D. Beylveled (2005)”, that there are no consequences for researchers who do not submit their research or fail to follow what the review requires. There are no circumstances in which ethics committee approval will render activities lawful that would otherwise be unlawful. Especially for the Ethics Advisory Board of VERITAS it is therefore important to monitor the respective trials/pilots.

#### 10.7.1 Summary of Bulgarian RECs

<b>Type of REC</b>	Central commission on ethics in drugs trials	Central commission on research ethics	Local commission on ethics in drug trials	Local commission
<b>Where situated?</b>	Ministry of health	Ministry of education & science	Regional hospitals	Universities & research institutions
<b>Who applies to them?</b>	Clinical trial proposals	researchers	Clinical trial proposals	researchers
<b>Formal/Informal</b>	Formal	Formal	Formal	Formal
<b>National/Regional</b>	National	National	Local	Local
<b>Laws Involved (see below)</b>	-Law on Drugs & Pharmacies (2000) -Regulation 26 of the Ministry of Health (1995) -Regulation 14 of the Ministry of Health (2000)	Regulations of respective ministries	-Law on Drugs & Pharmacies (2000) -Regulation 26 of the Ministry of Health (1995) -Regulation 14 of the Ministry of Health (2000)	Regulations of respective ministries
<b>Guidance Involved</b>	Declaration of Helsinki National Institute for Drugs - guidelines of Good Clinical Practice	Declaration of Helsinki	-Declaration of Helsinki -National Institute for Drugs - guidelines of Good Clinical Practice	Declaration of Helsinki
<b>Membership requirements</b>	At least 9 members, both medical & non-medical and of both sexes	At least 9 members, both medical & non-medical and of both sexes	At least 7 members, of whom no less than 1 is non-medical & 1 who is independent	At least 7 members, of whom no less than 1 is non-medical & 1 who is independent

			of applying hospital	of applying hospital
<b>Responsible/accountable to whom?</b>	To the Ministry of Health	To the Ministry of Education & Science	To the Central commission on ethics in drugs trials	To the Central commission on research ethics
<b>Approval or Advisory powers</b>	Approval	Approval	Approval	Approval

**Table 11 Summary of Bulgarian RECs.**

**Dataprotection Bulgaria:**

*Commission for Personal Data Protection*

*Mrs. Veneta Shopova*

*15 Acad. Ivan Evstratiev Geshov Blvd.*

*Sofia 1431*

*Bulgaria*

**Tel.** +3592 915 3531

**Fax** +3592 915 3525

**e-mail:** kzld@government.bg, kzld@cpdp.bg

The general principle of the patient's privacy is written in the Bulgarian health law. Personal data are described as "information for physical person which discloses his physical, psychological, mental, familial, economic, cultural, or social identity" (Article 2 of the Law on Data Protection). The law counts for living persons only. Anonymization process is not part of the law. In Article 21 it is written that an explicit written consent of the concerning person is used for processing personal data.

Article 19 says that the administrator has to inform the specific person about the aim and meaning of the data collection. Every participant has the right to correct or access his collected data. The Supervisory Authority does not have to be notified by data protection law in relation to medical research. The transfer of data needs to be approved by the Commission for Protection of Personal Data.

## **11 Detection and Management of Ethical Concerns of people affected by disabilities during the whole project phase**

During the first VERITAS workshop and user forum in Prague in Nov. 2010, a special issue was dedicated to present the Ethics Code of Conduct of VERITAS to a broad audience, to the other European projects partners (especially VUMS) as well to end-users and developers. The contact details of the Ethical Secretary were given to the audience. A thorough positive feedback from the audience was received regarding content, organisation and structure of the VERITAS Ethics Code of Conduct.

In order to empower especially the ethical concerns of the end-users, it will be discussed to enhance the Ethics Advisory Board by an end-user or by an end-user representative outside VERITAS. In addition to that an ethics side responsible will be trained on the special needs of the end users. The ethics responsables also have to fill out a questionnaire regarding any (ethical) concerns from the participants or any observations they made during the execution of the pilot/study/ experiment. If any breach of privacy or any other problem due to ethical principles will be reported, the EAB (Ethics Advisory Board) as well as the other pilot partners will be informed.

In addition to that, on the Informed Consent form the name and the contact details of the Ethical Secretary will be noted, so that the participants can report any threat to their personal wellbeing or integrity directly to the secretary. We regard ethical issues not as a state but as a process. Therefore iterative ethical design is a best practice approach as ethical problems sometime arise during the ongoing of the pilot and cannot be foreseen.

## 12 Conclusions

It is very important for us to highlight that the management of ethical issues follows a gradual approach. This means that the documents, such as this ethics Manual and the 'template on ethical and legal issues', will continuously be adapted to occurring ethical needs in this highly integrative field of research.

The Ethical issues under the auspices of VERITAS are listed within this manual. These are: Informed consent, privacy, risk assessment, the roles of the ethics advisory Board and the local Ethics Sites Responsible persons at pilot sites. Relevant information is summarized and is also being gathered throughout the questionnaire on ethical and legal issues.

The informed consent is a very important part of the research process; that is why a lot of space in the present manual is dedicated to this issue. The relevant facings of a valid informed consent for VERITAS are described. Since not all investigators might be familiar with compiling and the documentation of informed consent, two subchapters containing such information are added. No experiments are being performed with person unable to give a valid consent. The VERITAS user groups do not include mentally disabled people; only people with limited learning or cognition (i.e. memory or concentration or divided attention) difficulties, i.e. due to normal ageing.

Very important is that all private information is held confidential.

VERITAS research does involve experiments with human beings, as described in this manual. No human biological samples will be taken. The personal data will be strictly protected and unlinked anonymised. No genetic information will be collected. No user personal data and preferences will be centrally stored, nor sent around in the Network, nor will be available to any third party (i.e. for advertisement, marketing or even research – outside VERITAS objectives). All personal data recorded will only be locally stored on the device of the mobility impaired user. The goal of this manual is to compose a guide for all the researchers within VERITAS.

## References

- American Psychological Association (2002). Ethical Principles of Psychologists and Code of Conduct. *American Psychologist*, 57, 1060-1073.
- Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., Rohs, M., (2005). Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous computing, In: W. Weber, J. Rabaey, E. Aarts (Eds.): Ambient Intelligence. Springer-Verlag. Pp. 5-29.
- Charter of fundamental rights of the European Union. (2000) Nice.
- 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.
- Committee of Ministers Council of Europe ( 1990). Recommendation (No. R(90)3).
- Data Protection Working Party (2000). Privacy on the Internet – An integrated EU approach to On-line Data Protection, 5063/00/EN Final.
- Directive 95/46/EC of the European parliament and the Council (1995). On the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- 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.
- 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 2002/58/EC of the European Parliament and the council concerning the processing of personal data and the protection of privacy in the electronic communications sector.
- Disability Rights Commission (2004). Guidelines for Ethical research.
- European human rights convention (1950)
- 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.
- Kemppainen, E. Moral and Legislative Issues with regard to Ambient Intelligence. National research and Development Center for Welfare and Health (STAKES), Finland.
- Knapp, S. & VandeCreek, L. (2003). A guide to the 2002 Revision of the American Psychological Association's Ethics Code. Professionell Resource Press, Sarasota Florida.
- Medical Research Council (1993). The ethical conduct of research on the mentally incapacitated, London.
- Medial Research Council (2000). Personal information in medical research. In: Manual for Research Ethics. S. Eckstein (eds.). 367-390, University Press, Cambridge.
- OECD (1980). Guidelines governing the protection of privacy and transborder flows of personal data.
- Patry, P. (2000). Experimente mit Menschen. Einführung in die Ethik der psychologischen Forschung. Hans Huber. Bern.

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.

Warren, S. & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(1): 193-220, December, 1890.

World Medical association (2004). Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Participants, Tokyo.

# Annex 1 Questionnaire on ethical and legal issues

## SEVENTH FRAMEWORK PROGRAMME



Grant Agreement No. 247765

<b>Title</b>	VERITAS Questionnaire on ethical and legal issues
--------------	---

<b>Authors &amp; companies:</b>	Marcel Delahaye (COAT)
<b>Relevant Activity:</b>	4.1.5
<b>Summary:</b>	This is a tool to monitor and record the personal data handling within VERITAS
<b>Status:</b>	F
<b>Distribution:</b>	All Partners
<b>Document filename:</b>	-
<b>Version no.</b>	V1
<b>Issue date:</b>	20/04/2010

Is your experiment approved by a local research ethics committee?

- Yes
- No

If **yes**, please continue with question 1.

If **no**, please contact the Secretary of the Ethics Advisory Board.

***Informed consent clarifications***

Note: if private information is recorded, please use the additional documents ‘VERITAS informed consent template’ in ANNEX II and VIII “VERITAS Questionnaire on Personal information”.

1. Do you conduct experiments with **mentally** incapacitated participants (people unable to understand the informed consent form)?

- Yes
- No

If **yes**, **no experiment will be performed.**

If **no**, please continue with 2.

2. Is there any doubt about the individual’s mental capacity to consent?

- Yes
- No

If **yes**, **no experiment will be performed.**

If **no** please continue with 8.

3. a) Is the informed consent provided in very simple language

- Yes
- No

If **no**, why not?

.....

.....

.....

.....

b) Will the participant be given a lot of time to reflect his/her decision of giving or withholding consent?

- Yes
- No

If **no**, why not?

.....

.....

.....

.....

4. Is the participant unable to consent?

- Yes
- No

If **yes**, no experiment will be performed.

If **no**, please continue with 9.

5. Does the participant included in research object or appeal to in either words or action ?

- Yes
- No

If **no** (no objection) please continue with 6.

**If yes (he/she does object) no experiment will be performed!**

6. Is the participant unable to read the form?

- Yes
- No

If **yes**, please continue with b)

If **no**, please continue with 7.)

b) There are a range of people who are unable to read the consent form; these include those who have a severe visual problem, those with severe dyslexia, those who are illiterate and those whose knowledge of the language may be limited (e.g. a recent immigrant). For these people the information will be provided in appropriate alternative media (e.g. large print, audio tape, braille).

7. Is the participant deaf?

- Yes
- No

If **yes**, please continue with b)

If **no**, please continue with 8.)

b) The information has to be provided to the participant in a modality with which he is able to understand the informed consent form information (e.g. in written form)!

An oral explanation of the informed consent is not appropriate.

8. Is the participant illiterate?

- Yes
- No

If **no**, please continue with 9.

If **yes**, please note that the informed consent information has to be provided in a modality that the illiterate participant is able to understand (e.g. the statements have to be read to the participant) the informed consent form information.

The participant has to give oral consent which has to be witnessed at least by one person.

Informed consent form 3.4 has to be used.

**Legislation**

9. Is an oral consent of an illiterate participant that is witnessed in accordance with your national legislation?

Please comment:

.....

.....

.....

.....

.....

.....

10. Is there an international or national legislation, which you must follow when performing tests?

a) with healthy and able-bodied human participants?

Yes       No

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

.....

.....

.....

.....

.....

.....

.....

.....

.....

b) with participants with cognitive impairments / learning difficulties?

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

.....

.....

.....

.....

.....

.....

.....

.....

.....

c) with blind, deaf, motor disabled or illiterate participants?

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

.....

.....

.....

.....

.....

.....

.....

.....

.....

**Ethical control instruments**

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

- Laboratory or workgroup
- Division or department
- Institution
- Regional
- National

**12. Is there an ethics controlling body in your country?**

- Yes
- No

If **Yes**, please give details about the procedure:

.....

.....

.....

.....

**13. Is there a local ethics controlling committee, that your organisation is obliged to get approval from, for the experimental procedures before beginning with the experiment?**

- Yes
- No

If **Yes**, please give details about the procedure:

.....

.....

.....

.....

**14. Is there an established ethical control procedure which you must follow before performing tests with**

a) human participants?

- Yes
- No

If **Yes**, please give a brief description of it:

.....

.....

.....

.....

.....

.....

.....

b) with human participants with cognitive impairments / learning difficulties ?

If **Yes**, please give a brief description of it:

.....

.....

.....

.....

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

c) with blind, deaf, motor disabled or illiterate participants?

If **Yes**, please give a brief description of it:

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

**Privacy**

**Please note:** If private information will be recorded, the VERITAS informed consent template – to be found in the annex VIII, has to be filled in and signed by the participant and the investigator.

**15. Is private information recorded?**

- Yes             No

**If yes, please use also the informed consent template concerning private information.**

**If no, please continue with question no. 16.**

**16. Is there an established Data Protection Authority which you must follow before performing tests with human participants 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?

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

**17. Do you follow written procedures for protecting 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?

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

**18. Do you follow or are aware of any official national or international guidelines on protecting privacy?**

- Yes             No

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

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

**19. 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.

.....  
.....

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

**20. Do you identify persons and their professions who are authorised to have access to the data collected?**

Yes             No

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

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

**Safety**

**21. Will you provide information to the participants if you get aware of an illness?**

Yes             No

If **Yes**, please give a brief outline of it and provide some references

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

**22. Is every experiment evaluated for any side-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?

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

**23. Do 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?

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

**24. Do have written procedures for safety for 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?

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

***Risk assessment***

**25. Do you have procedures to perform risk-assessment concerning breach of privacy, and safety?**

Yes                       No

If **Yes**, please give a brief outline of it:

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

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

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

**26. Is your organisation insured against risks as a result of breach of privacy and safety?**

Yes                       No

If **Yes**, please give a brief outline of it:

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

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

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

**27. For conducting research and manage the risk, do you need to involve other organisations (unit, division, department etc.) that also control your research activity?**

Yes                       No

If **Yes**, please give a brief outline of it:

.....  
.....

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

## Annex 2 VERITAS Informed consent form template

### 1. GENERAL INFORMATION

*This part will be pre-filled by the investigator for each study.*

The VERITAS Ethics Advisory Board reviewed this pilot study from the standpoint of the protection of human research participants. The VERITAS 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 VERITAS Ethics Advisory Panel on:**

**1.3 Names of the investigators responsible for this project:**

### 2. INFORMATION ON THE RESEARCH STUDY

*The following issues should be explained (orally) by the investigator for each study to the participant before beginning 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?**

- What kind of data will be recorded, stored and why?

**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?**

- To whom will the data be transferred?
- How long is the length of storage?
- Where data will be stored, - according to which national legislation?
- Who will access the data?
- Who will supervise the data protection?
- How has the data ownership?
- Is the data connected to other information?

**2.9 What kind of benefits can I expect personally from taking part in this study?****2.10 What kinds of benefit to others can come out of this study?**

- Will the data possibly commercially exploited?

**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 Investigators' confirming statement**

*This part will be filled in by the investigator.*

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

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: \_\_\_\_\_

**3.2 Research participant's identity (participant unable to read the form; to be provided in a appropriate alternative media e.g. large print, audiotape, braille)**

*this part will be filled in by the participant.*

*The original will be kept be the investigator; 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: \_\_\_\_\_

**3.3 Participant Consent Form (participant unable to read the form; to be provided in a appropriate alternative media e.g. large print, audiotape, braille)**

*this part will be filled in by the participant.*

*The original will be kept be the investigator; a copy will be given to the participant.*

Title of the study:

\_\_\_\_\_

Place of the study:

\_\_\_\_\_

	<b>Please circle as necessary</b>	
	<b>Yes</b>	<b>No</b>
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.		
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.		
I was informed about the of any benefits to me or to others which may reasonably be expected from the research.		
I was informed about the explanations on confidentiality (and limits) of the data.		
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.		

I was informed about whom to contact for questions about the research and research participants rights.	<b>Yes</b>	<b>No</b>
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.	<b>Yes</b>	<b>No</b>
I understood and agreed with the handling of incidental findings.	<b>Yes</b>	<b>No</b>
I had sufficient time to take my decision.	<b>Yes</b>	<b>No</b>
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.	<b>Yes</b>	<b>No</b>
I have spoken to: <span style="float: right;">Dr./Mr./Ms.</span> .....		
I understand that I am free to withdraw from the study <ul style="list-style-type: none"> <li>◆ at any time</li> <li>◆ without having to give a reason for withdrawing</li> <li>◆ and without affecting my future medical care</li> </ul>	<b>Yes</b>	<b>No</b>
I agree to take part in the study.	<b>Yes</b>	<b>No</b>
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.	<b>Yes</b>	<b>No</b>
If aftereffects appear, I will contact Dr./Mr./Ms. ..... <b>with the tel. no.</b> .....		

Signed .....

Date.....

Name (in block letters).....

**3.4 Informed Consent documentation for an illiterate participant**

*This part will be filled in by the witness accepted by the LREC. The original will be given to the witness accepted by the LREC; a copy will be kept by the investigator.*

I confirm that I was present when the trial was conducted with the participant ..... The participant has given oral informed consent to the following points:

- The purpose of the research, expected duration, and procedures;
- the possible risks, discomfort, adverse effects, and side-effects (if any)
- a description of any benefits to the subject or to others which may reasonably be expected from the research
- confidentiality (and limits) of the data;
- Their right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing.
- contact for questions about the research and research participants rights.

I think it is appropriate to conduct the trial with the participant

.....

**Witness's Name:** \_\_\_\_\_

**Witness's Signature:**\_\_\_\_\_

**Date:** \_\_\_\_\_

## Annex 3 Organisational and insurance issues

### QUESTIONNAIRE FOR ORGANISATIONAL & INSURANCE ISSUES

*Explanatory Notes:*

- 1) *In the questionnaire with the term “interviewee”, we mean the potential users that participate in workshop, interview, presentation, focus group, pilot, and trial and they are asked to provide their feedback.*
- 2) *This part of the questionnaire is based mainly on the analysis made at the section of “Organisational and Insurance issues” within the main body of the Ethics Manual and reference on that is suggested in order to help the respondent (VERITAS partner) to answer the required questions adequately:*

#### **Organisation (Respondent) Details**

Company Name:  
 Contact Name:  
 Country:  
 Main Activity:

*Experience in involving interviewees in research: (Please elaborate)*

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

#### **Accessibility of facilities**

1. *Are your premises accessible and adequate for organizing workshop, interviews, presentation or focus group?*

Yes                       No

*If your answer is Yes, please give more details:*

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

*If your answer is No, please give reasons why not:*

.....  
 .....

2. *Do you foresee any special facilities for invited disabled people, when you organize a workshop, interview, presentation, focus group?*

Yes                       No

*If your answer is Yes, please give more details:*

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

If your answer is No, please give reasons why not:

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

3. Do you foresee to avoid small typefaces for your printed material that is addressed to people with disabilities?

Yes  No

If your answer is Yes, please give more details:

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

If your answer is No, please give reasons why not:

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

**Reimbursement Schemes**

4. Are there any standard surveys that your organization conducts where reimbursement or incentive payment is not introduced?

Yes  No

If your answer is Yes, please give more details:

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

If your answer is No, please give reasons why not:

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

5. Do you involve respondents who are being interviewed during their working hours and within their professional obligations?

Yes  No

If your answer is Yes, please give more details and specify whether you seek to gain their employer's permission first:

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

If your answer is No, please give reasons why not:

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

6. In case of incentive payments applied by your organization, do you introduce an Invitation to Tender (ITT<sup>1</sup>).

Yes  No

If your answer is Yes, please give more details:

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

If your answer is No, please give reasons why not:

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

7. Are there any cases where your organization is legally obliged to introduce payment incentives for involving disabled people or persons in general as interviewees and testers in its research?

Yes  No

If your answer is Yes, please give more details:

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

If your answer is No, please give reasons why not:

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

8. Are there cases (e.g. large amounts of incentive payments), where reimbursement scheme applied by your organization to interviewees may be considered remunerative work and affect any income benefit already received by the interviewee?

Yes  No

If your answer is Yes, please give more details:

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

If your answer is No, please give reasons why not:

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

9. Which is the amount in € that you usually apply in cases of incentive payments for  
a) survey interview .....€  
b) in depth face-to-face interviews .....€  
c) focus groups .....€

<sup>1</sup> For more info, please see relevant sub-section at Organisational and Insurance issues of the Ethics Manual.

- d) a full day workshop .....€
- e) other ..... (please specify) .....€

10. In the cases where you haven't conducted some of the above activities, please specify below the amount that you believe should be given to interviewees for their participation at.

- a) survey interview .....€
- b) in depth face-to-face interviews .....€
- c) focus groups .....€
- d) a full day workshop .....€
- e) other ..... (please specify) .....€

10. Do you prefer to reward your interviewees with cash or with a gift voucher? Please give your reasoning for that.

In cash  with a gift voucher

If your answer is "in cash", please give your reasoning:

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

If your answer is "with a gift voucher", please give your reasoning for this selection:

.....  
 .....

11. Is there an insurance provision that your organization should apply when they involve interviewees participating in trials?

Yes  No

If your answer is Yes, please give more details as well as reference laws:

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

If your answer is No, please give reasons why not:

.....  
 .....

**Links with related communities and authorities**

12. Do you develop links with local community groups, organisations and schools, in order to reach a wider pool of potential interviewees?

Yes  No

If your answer is Yes, please give more details:

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

*If your answer is No, please give reasons why not:*

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

*13. Is there a Local Research Ethics Committee, or a Social and Medical Funds and/or Occupational Health Authority in your country that should be consulted before initiating any trial with disabled people?*

Yes                       No

*If your answer is Yes, please give more details:*

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

*If your answer is No, please give reasons why not:*

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

## **Annex 4 Instructions for communication with deaf people**

1. In case that we don't know Sign language we call for a Sign language interpreter if it is necessary.
2. When we communicate with a deaf person we should have eye-contact with him (her). We have to speak slowly, distinctly (not loudly) with clear lips' movements avoiding to cover the view of the mouth.
3. When we want to be paid attention by a deaf person we touch gentle his(her) shoulder or we wave our hand in front of him(her)
4. We never touch the signer's hand when he is talking (signing).
5. During our conversation with a deaf person it's absolutely necessary to be at an enough lighted place. The light source shouldn't be behind the speaker.
6. We always inform the deaf person that we intent to leave the room.
7. When deaf people communicate we never interrupt them by passing or standing between them.
8. Deaf people should have their seats on the first rows, so in this way they can see maximum well.
9. Do not turn your head while you have a talk with a deaf person, and in case you have to do it explain the reason.
10. We have to respect the culture and the community of the deaf people.

## Annex 5 Interviews with disabled people - guidelines

Following on from the Manpower Working with Disabilities Report, we are proud to provide you with the Manpower Interview and Recruitment Guidelines aimed at the employment of people with disabilities.

As with the Working with Disabilities Report, the Interview and Recruitment Guidelines are primarily aimed at employers, as an informative and above all practical guide to interviewing and recruiting people with disabilities.

### Recruitment Advertising

- Consider advertising in disability-related publications and through disability support groups and charities.
- Consider job design carefully and do not require qualifications that cannot be justified by the job in question.
- Ensure that details of location are included as these may impact on whether or not certain candidates with disabilities apply for a job.
- Indicate the availability of flexible working conditions, if these are to be offered.
- Do not require any more of a person with a disability than would be required of anyone else.
- Include credentials as equal opportunities employer, if applicable.

### Setting up Interviews

- Expect the same measure of punctuality from applicants with disabilities as from applicants without disabilities.
- When setting up an interview time, consider the distance, weather conditions and physical obstacles that the interviewee may be presented with, and ensure that the interviewee is aware of how much time may be needed to arrive at the interview location.
- Be aware that an interviewee may need to arrange to be picked up after the interview has concluded - provide a good estimate of how long the interview will last.
- Visual disabilities: when giving directions, use very clear specifics including estimated distances where possible, for example, "turn right coming out of the lift and it's about five metres to the office door."
- Familiarise the interviewee in advance with the names of all people that will be met during the visit.
- Location: the proposed interview site should be reviewed to ensure it is accessible and appropriate for interviewing a person with a disability. Some important things to consider are:
  - availability of disabled parking spaces
  - ready access to public transport systems
  - ramp or step-free entrance
  - accessible toilets
  - accessible lifts, where relevant
  - clear signage on outside identifying the premises
  - layout of interview room – does it interfere in any way with the mobility of the interviewee?

- If any of these are inadequate and alterations cannot readily be made, inform the interviewee of them prior to the interview and offer to arrange an alternative interview site.

### **Meeting and Greeting at Interviews**

- Use a normal tone of voice when extending a welcome.
- Shake hands, even when a person may have limited hand use or an artificial limb. A left-hand shake is acceptable. If the person cannot shake hands, touch the person on the shoulder or arm to welcome.
- Look and speak directly to the interviewee rather than to any companion, helper or interpreter that may be present and maintain eye contact with the interviewee.
- Offer assistance with dignity and respect and be prepared to accept instructions.
- Allow a person with a visual impairment to take your arm (at or around the elbow), allowing you to guide rather than force.
- Offer to hold or carry packages in a respectful manner.
- Do not offer to handle a cane or crutches unless requested and do not lean on a wheelchair.
- Do not patronise wheelchair users by patting them on the shoulder.

### **Conducting the Interview**

- Do not ask questions that would not be asked of a person without a disability in similar circumstances, for example:
  - do not ask how the disability was acquired
  - avoid focusing on the disability unless it is the only way to find out what adjustments are required.
- Eliminate any medical questions that are not strictly justified by the inherent requirements of the job ... and do not impose medical checks on interviewees with disabilities that would not be applied to interviewees without disabilities.
- Ask what requirements may be needed to enable the person to do the job comfortably and be prepared to discuss how to cater for any difficulties that might be envisaged.
- Treat the person with the same respect you would treat any applicant.
- Assume the interviewee is of normal intelligence.
- Always look and speak directly to the interviewee.
- Do not be embarrassed if a common expression which relates to the interviewee's disability is used, for example, "see you later" with a visually impaired person.
- Be willing to repeat questions and if not understood a second time, ask in another way.
- Show patience when speaking and listening.
- Do not pretend to understand if you are having difficulty doing so - do not be embarrassed to ask for clarification.
- Do not touch the person in overly familiar ways, unless you are familiar with them.
- Common mistakes: openly admiring the applicant's courage, expressing sympathy, staring or avoiding eye contact, avoiding essential questions, assuming help is needed, asking about "your handicaps".

- Refer to “non-disabled people” or “people without disabilities” rather than “normal” people.
- Ask about any special equipment or reasonable adjustments that may be required should the person be successful in getting this job.

#### MOBILITY

- Keep crutches, canes or wheelchairs within reach of the interviewee.
- Some wheelchair users may prefer to sit in an office chair for the interview.
- When speaking to a person in a wheelchair or on crutches for more than a few moments, sit down to be at that person’s eye level.

#### SPEECH IMPAIRMENTS

- Give the interviewee complete attention.
- Be encouraging rather than correcting; do not adopt a concerned expression.
- Ask questions that require short answers or a nod of the head.
- Resist the temptation to speak for a person who is having difficulty expressing themselves; do not raise your voice.

#### VISUAL IMPAIRMENTS

- Identify yourself and introduce anyone else present.
- If the interviewee does not extend a hand shake, express a verbal welcome.
- When offering seating, place the interviewee’s hand on the back or arm of the chair and provide a verbal indication.
- Indicate in advance before moving from one place to another.
- Let the interviewee know when the conversation has ended.
- If interviewing in a group situation, provide a verbal indication by announcing the name of the person being addressed.
- Do not feed, pat or distract a guide dog.

#### HEARING IMPAIRMENTS

- Find out before the interview if the interviewee will rely on lip reading and be sure to face the person during the interview and when guiding around the interview site.
- Ensure that the interview room is quiet and that outside disturbances, such as traffic noise, are minimal.
- Be prepared to write a message if being understood becomes difficult.

#### **Work Environment**

- Consider whether any physical feature of the workplace puts disabled people at a substantial disadvantage and, if so, make the necessary reasonable adjustments.
- Remember that access for wheelchair users is not the beginning and end of the story.
- Examples of how to improve accessibility include:
  - removing clutter from common areas
  - painting doors a contrasting colour to walls for visually impaired workers

- lowering light switches for wheelchair-users
- considering modifications to equipment, for example, visible as well as audible fire alarms for deaf workers.
- Consider what assistive devices could be introduced, for example, a computer with speech output and provide training in their use.
- In managing work schedules, consider whether it is reasonable for adjustments to be made to accommodate disabled employees, for example, flexibility in leave arrangements for workers whose disability requires periodic treatment.
- Be prepared to reallocate minor duties to another employee.
- Make instructions and manuals accessible, for example, a Braille version for the visually impaired.
- Prepare non-disabled employees on any adjustments needed for working with disabled colleagues.

**In General:**

- Put the person first and disability second.
- Do not make assumptions about the disabled worker's needs.
- Remember that some disabilities are hidden.
- Talk to each disabled person about individual needs.
- Look into what help is available.
- Introduce disability issues specifically into equal opportunities policies and monitor effectiveness.
- Consider whether you need expert help to assess the needs of the individual and to find out about the range of adjustments that can be made.
- Consult other employees to win buy-in for any changes proposed, but seek the permission of the disabled employee before consulting others about anything specific to that individual.
- Consider disabled workers in plans for career progression and training.
- Allow absences during working hours for rehabilitation, assessment or treatment.
- Position disabled employees' work stations in places that offer the best accessibility.
- Plan ahead. Think now about what can be done costeffectively to anticipate future legislative requirements.

## Annex 6 Communicating with blind and partially sighted people

**Summary:** Information about ways of communicating with blind and partially sighted people.

Communication means with blind and partially sighted people:

- Print
- Braille
- Moon
- Magnifiers and access technology
- Internet
- Audio tape
- Personal readers
- Telephone
- Word of mouth
- Deaf blind people
- People with additional disabilities
- Ethnic minorities
- Further information

---

Blind and partially sighted people have the same information needs as everyone else. But many people with sight problems will not be able to understand information unless it is made available to them in a suitable format. It is important to remember that there is no single method which suits all blind and partially sighted people all of the time. Even the same person will use different methods at different times and under different circumstances.

### ***Print***

Nearly half of all people with sight loss can read ordinary print, but only with great difficulty. Reading a long document can be laborious, slow, and exhausting. The main advantage of ordinary print is that information is widely available in this format. The main disadvantage is that most people with a sight problem can't easily read it.

Many people, especially those who have lost their sight in later life, can still write by hand, even if they can't read what they have written! This problem can be solved for some people by printing each character, using a thick black marker pen in order to make it clearer.

Signing documents and filling in forms can also be difficult, especially when they can't see where on the form they are supposed to write. This first problem can be solved by the use of signature guides which show the blind person where to sign. The latter can be solved by designing more legible forms.

### ***Clear print***

Clear Print is an approach to designing and producing your printed materials which takes into account the needs of blind and partially sighted readers. Simply, a Clear Print document will find a wider audience. The solutions we propose are straightforward and inexpensive, focusing on some basic design elements, for example font, type size, contrast and page navigation. By following our guidelines, cutting edge design can also be inclusive design.

Clear Print differs from large print in the size of the type used (known as point size). Clear Print documents use a minimum type size of 12 point (although RNIB recommends 14 point to reach more customers with sight problems). Large print documents are produced in a larger type size, ranging from 16 to 22 point.

### ***Large print***

For many blind and partially sighted people, larger print is essential. No single size is suitable for everyone but most people prefer their large print in the range of 16 to 22 point. If possible, for example with personal communication, always ask your customer which size best suits their needs. You can produce simple large print documents yourself in-house, but more complex jobs may need to be sent to a commercial printer. More information on producing large print is available in our See it Right pack.

### ***Braille***

Braille is a system of raised dots which people can read with their fingers. Many blind and partially sighted people prefer particular types of information in Braille, for example information to be used in meetings or to be read silently.

Braille may be produced in-house if you have the right software, training and an embosser (Braille printer). It is more common for it to be produced by a transcription agency.

For more information on producing Braille see our See it Right pack.

### ***Moon***

Moon is a system of reading and writing in which tactile symbols based on lines and curves are used to represent letters, numbers and punctuation marks. Moon is used by a very small number of people, most of whom are elderly. The advantages of Moon over Braille are that the system is easier to learn, the letters are easier to distinguish by touch, and it is easier for sighted people to understand. The main drawbacks of Moon are that it can't be written by hand, it is even bulkier than Braille and there is very little literature available.

### ***Magnifiers and access technology***

There is a wide range of equipment which can be used by blind and partially sighted people to help them access information:

- simple hand-held magnifiers
- Closed Circuit Televisions (CCTVs) which magnify print up to 48 times the original size
- speech software which can read the computer screen to the user
- Braille translation software which can translate information on a computer screen into Braille that the user reads on a specially adapted keyboard
- screen enlargement software that enables the user to magnify the text on their screen to a suitable size.

The advantages and disadvantages of each type of equipment depend on the type of equipment, as well as the manufacturer and model. Generally speaking the more hi-tech a device the fewer people who are likely to use it. Most blind people prefer low-tech devices. There are a number of reasons for this including fear of new technology, lack of training, lack of money (most hi-tech devices are very expensive) and the fact that hi-tech devices are not always appropriate. Many blind people, for example, prefer to listen to a human being rather than a mechanical voice. This said, hi-tech devices offer exciting new opportunities for some people with impaired vision to communicate on a level with sighted people.

### ***Internet***

The internet is one of the most significant communication developments since the invention of braille. For the first time ever, many blind and partially sighted people have access to the same wealth of information as sighted people and on the same terms.

For example, a blind internet user anywhere in the world can now read today's issue of The Times, locate the best restaurants in Paris or search records in the Library of Congress, in exactly the same way as a sighted person might.

However, to enable people using this technology to access information on a website, the website must be correctly designed. Information on designing accessible websites is available from the Web Access Centre.

### ***Audio tape***

There are various kinds of cassette recorder/players available to blind and partially sighted people. Each has its own advantages and disadvantages. Age is the key factor in determining use with few people over 65 possessing a tape machine of any kind.

### ***Commercial cassette recorder/player***

There are several advantages to this type of tape recorder/player. They are widely available, they can be used to record information as well as to listen to it, and there is an increasing range of materials available on tape. The main disadvantages are that commercially available tapes are often abridged, the tapes are not marked for ease of use by people who can't see clearly, it can be

difficult to locate specific passages on the tape and many elderly people find the controls on the recorder/players too difficult to use.

### ***Easiplay cassette player***

There are a number of machines which have been designed to be as easy as possible to use. The Easiplay machine has a limited number of functions and all the keys are clearly marked with tactile symbols in contrasting colours. It is also sturdy and well marked. The disadvantages are that it is relatively expensive, the sound quality is poor and it cannot be used to record information by the user.

### ***Handi-Cassette player***

There a number of tape machines which have been designed for the more sophisticated user. The Handi-Cassette machine has a four-track function, a tone indexing facility, variable pitch and speed controls, and is lightweight and portable. Four track machines allow twice as much information to be recorded onto the same tape as an ordinary, two track machines. Tone indexing allows the user to mark specific points on the tape with an audible bleep or message, making it easy to locate when winding the tape at speed. Variable pitch and speed controls allow the reader to listen to the tape at a speed and pitch that suits him or her. The disadvantages of these machines is that they are relatively expensive and many elderly blind people find them too difficult to operate.

### ***RNIB Talking Book Player***

RNIB's Talking Book Service is available to anyone who is blind or partially sighted. Members pay an annual subscription, for which they receive a Talking Book Player and as many books as they can read whenever they want them. There are several advantages to RNIB Talking Books. The Player is sturdy and easy to use, with free servicing by a local Talking Book volunteer. The books are recorded onto six track tapes, with a playing time of up to twelve hours, which means that an entire novel can be recorded onto a single cassette. There is a wide choice of books, with over 10,000 titles currently available. Books are delivered and returned, free of charge, by post. There are a few disadvantages. Members have to pay an annual subscription fee (although this is often paid by the local authority), the Player is not as portable as some of the more lightweight machines, ordinary commercial cassettes cannot be played on the Player and the Player cannot be used to record information by the user.

### ***Personal readers***

Many people with sight problems use other people to read to them on a regular basis. The advantage of using another person to read to you is that it is simple and effective. A drawback is that you have to rely on the other person and you may not wish someone else to read materials which are private or confidential.

### ***Telephone***

The telephone is a lifeline for many people with sight problems, especially those who can't get out by themselves. The major plus point of the telephone is that people can ring other people, instead of relying on other people to come to them. The main disadvantage is that not all blind people can afford a phone and some blind people are also deaf or hard of hearing.

### ***Word of mouth***

Word of mouth is probably the most important method of communication used by people with sight loss. Its main advantage is that it is simple and effective. Its main disadvantage is that some blind people find conversation difficult because they can't make eye contact with the other person or read their body language. They may not even realise the other person is there.

If approach a blind person, say hello, who you are in case he or she doesn't recognise you or your voice. Address him or her by name, if you know it. If not, a light touch on the arm will indicate who you are speaking to. Before you move away, say that you are about to leave. Everyone feels foolish talking to an empty space.

### ***Deaf blind people***

There are around 23,000 people in the UK who have a severe loss of both sight and hearing. About 200,000 have less serious dual sensory loss. Some deaf blind people have enough hearing to use the telephone if background noise is kept to a minimum, and the caller speaks clearly and at a pace which suits the individual. Other deaf blind people use text phones (or minicomms) or Typetalk, which is a free national relay service using operators. The deaf blind person uses a text phone to contact the operator and then the operator rings you and relays the message.

### ***Systems for deaf people***

Some deaf blind people retain enough sight to be able to use systems used by deaf people such as lip reading or British Sign Language or the Deaf Alphabet. It usually helps if the deaf blind person has the light to the rear so that he or she can see the other person's face and hands more clearly. The benefit of lip reading is that sighted people don't have to learn a new system although a drawback is that it requires a great deal of effort and concentration on the part of the deaf blind person. The disadvantage of British Sign Language and the Deaf Alphabet is that both parties have to learn the system. The Deaf Alphabet is quicker to learn than British Sign Language but the latter is much more flexible and faster to use.

### ***People with additional disabilities***

Many blind and partially sighted people have additional disabilities which may affect the manner in which they communicate. People with diabetes for example are less likely to be Braille users if they have lost the tactile sensitivity in their

fingertips. People with arthritis may find some cassette recorder/players too difficult to operate.

***Ethnic minorities***

People with sight problems from ethnic minorities may face additional communication difficulties. There is very little material available in large print or Braille or on tape in ethnic languages.

## Annex 7 Official definitions/principles applied

### ***From the Directive 95 / 46 / EC***

#### **Article 2**

##### Definitions

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.

## **OECD privacy principles**

We abide to the principles mentioned below:

### **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".

Within VERITAS personal data will solely be disclosed to other parties with the consent of the participant.

### **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".

We will meticulously protect the infrastructure, where personal data is being stored. The next chapter about Security issues within VERITAS covers this topic.

### **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 have 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.

## ANNEX 8 Questionnaire on personal information

### SEVENTH FRAMEWORK PROGRAMME



Grant Agreement No. 247765

<b>Title</b>	VERITAS Questionnaire on personal information
--------------	---

<b>Authors &amp; companies:</b>	Marcel Delahaye (COAT)
<b>Relevant Activity:</b>	4.1.5
<b>Summary:</b>	This is a tool to monitor and record the personal data handling within VERITAS
<b>Status:</b>	F
<b>Distribution:</b>	All Partners
<b>Document filename:</b>	-
<b>Version no.</b>	V1
<b>Issue date:</b>	20/04/2010

This document aims to explore the amount of gathering, recording and processing of personal data. We would like to ask all VERITAS partners (with training, study or pilot activities) to fill in the questionnaire ***who collect personal data*** – also in its broadest sense.

In accordance with the directive 95/46 CE personal data is defined as: '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;

### **Is personal data recorded?**

Yes       No

If **yes**, please describe and answer the questions below.

If **no**, the document at hand does not have to be filled in.

### **Description of personal data**

**recorded:**.....

.....

.....

E.g.

- *Name etc, linked to mobile device*
- *Video observations of persons*

### **General information:**

Partner name: .....

In which Workpackage or Activity is personal data collected?

.....

### ***Questions concerning personal data***

#### **1. What kind of data will be recorded, stored and why?**

Please comment:

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

E.g.

- *Name etc, for administration to use mobile device. Names for the administration and codes for the other personal data and test results will be stored separately.*
- *Video observations for evaluation*

**2. Will the data be transferred (e.g. to another country, to another organization or within the organization)?**

Please comment:

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

E.g.:

*Yes, to VERITAS project partner*

**3. Who owns the data copyrights (Data ownership)?**

Please comment:

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

**4. Is the data connected to other information? (e.g. databases)**

Please comment:

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

**5. Will the data be possibly commercially exploited?**

Please comment:

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

**6. For how long is the data being stored (Length of storage)?**

Please comment:

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

E.g.:

*During test and evaluation period of pilot tests*

**7. Where will the data be stored, - according to which national legislation?**

Please comment:

.....  
.....

**8. Who will access the data?**

Please comment:

.....  
.....

**9. Who will supervise the data protection?**

Please comment:

.....  
.....

# ANNEX 9: Ethical Pilot Application Form

to be submitted at the VERITAS Ethics Advisory board

Submitted at VERITAS Ethics Secretary am xx.xx.20xx

## Title:

- 1. application
- application

## Ethics Site Responsible

Name,:  
 Function:  
 Address:  
 Tel.:  
 Fax:  
 E-Mail:

## Sponsor

European Commission  
 SEVENTH FRAMEWORK PROGRAMME THEME 3  
 Information and Communication Technologies  
 Adresse: Rue de la Loi 200, B-1049 Bruxelles

## Description of the Pilot/Experiment/Study

.....

.....

.....

.....

## Ethical Considerations/ Benefit and burden of the Pilot/Experiment/Study

.....

Number of participants: \_\_N

## Participation of subjects who need special protection?

- no
- yes
  - healthy subjects
  - Underage
  - patients
  - people unable to give valid consent

- emergency patients
- patients who are in the proces of dying
- others:

### Multicenter study

Name of the other countries who take part in the study:

### Duration:

### Approval of the Local Research Ethics Committee

- yes, please attach approval
- no
- pendent

### Protocol: (short description)

Insurance: (*short description*)

.....  
.....

Date:

Name of the Ethics Site Responsible/ Signature:

**Error! Reference source not found.** .....

---

### Will be filled in by the Ethics Secretary

The Ethics Secretary confirms that the application has been approved by the VERITAS Ethics advisory bord

Marcel Delahaye: .....

Date: Signature: