ISITEP
D8.5.1 – DETAILED REPORT ON THE ETHICAL, LEGAL AND SOCIETAL ASPECTS OF THE PROJECT

Document Manager:	Federico Frosali	SES	Editor

Programme:	Inter System Interoperability for Tetra-TetraPol Networks
Project Acronym:	ISITEP
Contract Number:	312484
Project Coordinator:	Selex ES
SP Leader:	SES

Document ID N°:	ISITEP_D8.5.1_20150921_V3.0	**Version:**	V3.0
Deliverable:	D8.5.1	**Date:**	21/08/2015
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	Federico Frosali (SES)
Approved by (WP Leader):	Federico Frosali (SES)
Approved by (SP Leader):	Paolo Di Michele (SES)
Approved by (Coordinator)	Paolo Di Michele (SES)
Security Approval (Advisory Board Coordinator)	Etienne Lezaack (BFP)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
All the partners	All the company	Contributor

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
All Company Project Managers	All involved companies	Members of the Steering Committee
Elina MANOVA	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
V1.0	07/11/2014	All	All	First issue
V2.0	06/03/2015	All	All	Updated according to the remarks of the Commission
V3.0	21/09/2015	All	All	Updated according to the new remarks of the Commission

Terms and acronyms

Abbreviation	Definition
ELS	ethical, legal and societal
ICT	Information Communication Technology
IPR	Intellectual Property Right
ISITEP	Inter System Interoperability for TETRA_TETRAPOL Networks
WP	Working Package

PUBLISHABLE EXTENDED ABSTRACT

The objective of WP 8.5 is the development of a harmonized, agreed and realizable framework addressing ethical, legal and social (ELS) aspects of ISITEP.

In this deliverable an overview of possible issues applicable to ISITEP framework and arising from research activities are analysed.

Since the project deals with national security, public safety, crimes and disaster prevention and management, going further single national frontiers, special attention has to be paid to ethical, legal and societal implications of an instrument that permits operators of different nationalities to cross borders continuing to have available the same services that they had at home and, at the same time, to cooperate with foreign colleagues. The social impact of ISITEP framework and the benefits that can be drawn from its use, commensurate with possible drawbacks, give an evaluation of its compliance to basic principles of ethics, legality, and social sustainability.

This document analyses ethical, legal and societal issues which can involve ISITEP project development and the deriving interoperability framework, focusing on their correlation with the scope and the roles ISITEP intends to play in the modern European society. In particular, the document verifies:

- Compliance to *proportionality* and *subsidiarity* principles that permit to confirm the societal value of the project.
- Liability risks coming from an inadequate observation of legal requirements and from ISITEP framework misuse in international operative scenarios.
- Privacy aspects due to exchange of information between responders coming from different countries which could have different legal constraints on citizens' personal and sensible data exchange, or between responders of different agencies cooperating in a crisis scenario but having different tasks and different permission or interest in citizens' information.

A general analysis of these principles is applied to ISITEP through a list of questions addressing in detail ELS in the framework. A deepened characterization is obtained applying questions referring to PPDR forces cooperation through the interconnection of different European networks to use case scenarios chosen between ISITEP trials scenarios.

Since the ethics agreement reflects also a common, basic, not legally binding standard of conduit for the proper application of the project outputs, the second part of the deliverable examines ELS matters concerning the project development and the consortium. General considerations about respect for individual, privacy and data protection, information exchange, sustainability, and intellectual property are drawn and verified through a procedure to face ELS in ISITEP project development. This procedure uses a survey (see Appendix A) filled by all project-partners in order to maintain the transparency toward other partners, and eventually adjust the steps needed to reach solid long-term foundation in ethical, legal and social aspects.

CONTENTS

1. INTRODUCTION

The objective of WP 8.5 is the development of a harmonized, agreed and realizable ethical, legal and social (ELS) framework both for the development and establishment of cross-border operations enabling tools.

Technologies have a great effect on people security, moral and welfare. Hence, research projects, which inherently bring changes in the technologies currently used, leads to possible uncertainties potentially affecting people and their values; for this reason every innovation take on an ethical dimension.

Ethics constitutes a major issue particularly in research that involves health and biology, like as staminal cells, experimentation on laboratory animals, humans, etc. However, also research on ICT systems, even in an industrial environment, leads to ethical/political/legislative issues as arisen e.g. in the Communication of the European Commission: “decision-makers are constantly faced with the dilemma of balancing the freedom and rights of individuals, industry and organizations with the need to reduce the risk of adverse effects to the environment, human, animal or plant health” [1].

ISITEP project responds to one of the modern society and technological culture challenges, delivering a cross-countries solution for interoperability between first responder communications systems; since it attends to sensible topics related to public safety, it should be carefully regulated from an ethical and legislative point of view.

Hence in ISITEP project general principles of ethic (such as what people think is right, how people should act, how moral constrains can be put into practise respecting rights, obligations, benefits for society, fairness, etc.) merge with the specific requirements of the Public Safety environment with a clear impact on environment and society.

The ELS theme is vast and complex; it has facets and can be analysed from different point of view. In particular, in this document, two perspectives are investigated:

- ISITEP framework as such and its end-use;
- ISITEP Project development, in particular the approach of consortium members to research and development activities.

ISITEP framework is rather complex, so potentially source of many criticalities. For this reason, the first step is to try to contextualize the ELS problems to ISITEP identifying issues directly tied to ISITEP main characteristic that is the opportunity to make PPDR forces of various nationality fully cooperating and interoperable.

On the other hand, the second part of the deliverable is about the possible issues arising from research activities are therefore analyzed and a procedure to face the ELS during the execution of ISITEP project is outlined.

2. GENERAL PRINCIPLES

This document wants to examine the implications of moral and legal principles and practices in the project development and in the project results; ethic issues can be analysed considering two different but complementary perspectives.

The first perspective deals with ELS issues relative to the framework itself. From a general point of view, it is important to assess the impact that the introduction of such a framework could have on the society from an ethical and legal point of view. The starting point to conduct this analysis is represented by the needs of modern society to increase citizens' security, maximizing the efficiency and effectiveness of public safety operations. The use of such technologies could have either positive or negative consequences on society. In particular, pros and cons could have implications and correlation in the field of human rights, liability and privacy. Even though use contexts of this tool are very sensitive, we have to consider that the instruments constituting the framework are consolidated in the various European nations. The main innovation introduced by ISITEP resides in interoperability, hence possible relevant issues can arise when considering scenarios in which multiple agencies of different nationalities cooperate. The ISITEP ethical impact has to be evaluated under a broad perspective focusing on integration, cooperation, and adaptation of technologies, people and procedures.

The second perspective refers to the way to carry out the project, based on the common sense of "right and wrong" which prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, and specific virtues. In this case ethics concerns the right to work, the right to choose, the right to privacy, the right to freedom of expression (speech, religion…), and the right to no discriminations. To this goal Company ethical principles can be declared in a code of conduct intended to preserve and lead business integrity.

Another aspect of ethic deals with the project results and the output of the project, which must be based on honesty and impartiality:

- new and better results have to be pursued to improve the state of art in topic under evaluation;
- all outcomes have to be inspired by truth and integrity even in case of fallibility and inconclusiveness, avoiding arbitrary views and incoherence and refusing all forms of plagiarism;
- all subjects shall to inform partners, costumers and others of all possible conflicts of interest that exist or can arise during or after project conclusion;
- all achievements have to be supplied with verifiable documentation and to be subject to impartial discussion even in case of conflicting opinions;
- the originality and the usefulness of the project has to be clear and pursued in all phases of the project;
- responsibilities are shared between partners, that contribute each with own expertise;
- IPR is respected following a Consortium Agreement.

In addition to these aspects, also security issues are particular relevant for the project; for this reason specific WPs are dedicated to this topic (see for example WP 22, 46, 53) and technical details are not investigated here. Indeed ISITEP project is based on the seamless integration of TETRA and TETRAPOL networks with the goal to overcome the current operational and technological barriers and have connected infrastructures for public safety applications. A European network of network and agreed procedures will be used to communicate and store particularly critical data that must be exchanged in a secure manner, hence the project foregrounds must be carefully protected.

3. ETHICAL, LEGAL AND SOCIAL ISSUES IN ISITEP FRAMEWORK

This section analyses the ethical, legal and social aspects of ISITEP framework in the fields of human rights, privacy, data protection, and liability.

First of all, it is needed to focus the attention on the ISITEP project objectives.

ISITEP aims to developing procedures, technologies and legal agreements for achieving a cost effective solution for PPDR interoperability, through a framework composed by:

- Mission oriented procedures, functional models and legal agreements.
- A European network solution integrating all types of European national PPDR networks through a novel Inter System Interface (ISI) over IP protocol encompassing ETSI standardized ISI among TETRA national networks and ISI over IP gateways among national TETRAPOL-TETRAPOL and TATRAPOL-TETRA networks.
- Bi-technology terminals based on smartphones/tablets with PPDR applications.
- Supporting tools to assess business sustainability and technology needs and to improve training.

Hence, ISITEP main goal is to make interoperable systems that have been designed for the same use, with similar requirements and services, but based on different technologies. Nowadays, most of UE Countries have adopted one of the two PDDR communication system, thus leading to a jeopardized situation, making cross-country communications de facto impossible. However, networks interoperability, as foresees by the ISITEP project, will facilitate cooperation between Member States on both national and international level, with the aim to achieve quicker, safer, and more effective police operations. As a consequence, the main aspect that must be taken into account in the analysis of possible ELS issues is that the interoperability introduced by ISITEP project supports transnational operations and cooperation activities which, by definition, involve two or more countries, each claiming sovereignty and exclusive jurisdiction within its own borders.

In this context there are two other aspects that must be taken into account:

- the presence of Schengen Agreement, that are already in place in Europe;
- who the end-users of the framework are, and their role.

Schengen Agreement is well known for allowing the free movement of goods and persons between member states, but it also allows information exchange for international cooperation (as operational data or cross-border observation) and provides the installation of communication means (telephone, radio) for the connection of border office with the authorities of member states [see Schengen Convention, supra note 66, arts. 39-91].

Two articles of Schengen Agreement are at the basis of cooperation among the police authorities of different contracting states:

- Article 39 obligates police agencies of member states to provide information, upon request, for mutual assistance in prevention or detection of criminal offenses.
- Article 46 permits the free exchange of information that may help to prevent future crimes or public order issues.

Moreover Schengen Agreement enables national police to access information about missing or wanted persons, individuals refused entry, and stolen properties. This is also extended by European Directive 2011/99, which sets the rules enabling a judicial or equivalent authority in a Member State, where protection measures are adopted for protecting citizens against criminal acts; this allows a competent authority of a member state to continue protection activities cross-border and in the territory of other member states, safeguarding citizens physical or psychological integrity, dignity or personal liberty.

The second aspect concerns the end-use of the ISITEP framework. The project aims to develop procedures, technologies and legal agreements to have a global solution for PPDR interoperability across Europe directly involving also the end-users. This allows a strong correlation between the ISITEP project developments and the use of its outputs. This is confirmed by foreseen demo scenarios (see SP7 documents):

1. multi agency (bus accident),
2. police hot pursuit,
3. airplane disaster in Geneva border,
4. joint police surveillance patrol,
5. VIP protection service.

These examples suggest that ISITEP use can vary depending on the application context. In any case, in general, involved parties come from different countries that can have different legal, cultural and technological backgrounds. Moreover, ISITEP framework users are heterogeneous (e.g. police forces, but also rescue teams, first medical aid operators, professional operators) and are interested or restricted to exchange only some type of information, These remarks should be taken into account when general ELS principles are contextualized to ISITEP framework. In particular this document will focus on trials scenarios which represent the first actual implementation of interoperability between different countries and agencies, in order to provide a deep analysis of the ELS issues.

ELS issues in ISITEP are directly tied to its end use that does not basically differ by current policies and purposes of TETRA and TETRAPOL use, since ISITEP focuses only on their integration aimed to improve performance and efficiency in operative scenarios enabling new fields of application. Cross-countries use scenarios and interoperability, which are the real innovation introduced by ISITEP, lead to consider that the main involved ELS aspects are related to communications' security and data protection. Although personal data treatment is regulated by European directives and national laws and procedures, some new concerns could arise since multiple and different nations and subjects are involved; this implies the possibility to resort to particular agreements or operators' training. Moreover, security has to be guaranteed at different levels, from communication links confidentiality to access control.

3.1. HUMAN RIGHTS AND ETHICAL

Human rights and ethical analysis permits to legitimate the ISITEP framework, and to assess its compliance to European Convention to Human Rights. Following the path traced by Virtuoso [2] and IDECT [3] project before, it appears important to substantiate the played role, the pursued purposes and the produced improvements of ISITEP framework in the modern society. From an ethical point of view, particular interest can be paid to the principles of *proportionality* and *subsidiarity*, which verify the societal value of the project, confirming that, in achieving its goals, the framework uses means proportionated to its objectives and as least invasive as possible.
Societal value of ISITEP outcomes lies in its main purpose of increase the efficiency of critical and security operations that involve citizens and resources in European countries. One of its most relevant characteristics is the attempt to increase countries integration and collaboration in respect of single states' laws and cultural differences.
The outputs of ISITEP project aim to extend the cooperation capabilities of existing and wide adopted communication systems to allow transnational cooperation.

Making citizens aware of ISITEP efforts and purposes contributes to increase people confidence in authorities and public service organizations, together with the awareness to can rely on a more concrete and organized support from public authorities. Moreover, ISITEP can be seen as a deterrent instrument.

This can be better explained by an example in which a criminal commits a crime and tries to escape across country borders counting on that he won't be followed or he can take advantage from the inefficient cooperation between polices due to long and complex communication procedures. If police forces of all countries can rely on a unique framework the communication can be direct and immediate facilitating the operations. This can contribute to reduce delinquency and make the citizens fill more secure.

Hence we have to ask if ISITEP project follows proportionality and subsidiarity principles, adequately informing citizens about its purposes, achievements and efforts. This and further points will be addressed through the questions validating the ELS guidelines applied to ISITEP framework use scenarios in section 4.

3.2. LIABILITY AND FORESEEABLE END-USE

Liability risks emerge when legal requirements are not correctly adhered or when insufficient measures have been taken to prevent misuse of ISITEP framework, eventually causing damages.

The first aspect is that ISITEP project involves subjects coming from different nations, with different cultures and subject to different national laws, in addition to the common European Directives. Moreover, due to great flexibility of the framework, the application scenarios can differ significantly in location, involved subjects (e.g. operators, disaster victims, crime perpetrators, etc.); for this reason it is difficult to identify, foresee and address all possible risks connected to the end use of ISITEP framework. From a legislative point of view, European directives as well as legislation of the country in which event occurs shall be followed. When the operation is performed across nation boundaries specific agreements may be required. Hence, the question is if and which kind of agreements are needed to guarantee liability.

Moreover, while proper design of ISITEP framework is mainly responsibility of its developers, large part of liability deriving from its use has to be ascribed public safety agencies and national network owners. It is by the way essential to consider ethical and human issues in the project development stage to reduce the risk of possible infringement in the stage of actual use and foresee adequate informative process for end-user about liabilities that they could face to.

We have to underline that ISITEP outputs aim to add interoperability to current PPDR communications capabilities. The legal aspects are already addressed and consolidated in each country. Liability of ISITEP is safeguarded by the presence of end users in the consortium or in the advisory board, guaranteeing that ISITEP really respects users' needs, harmonizing the framework towards legal and single national operative contexts.

The problems can arise if an unauthorized or improper use of some framework functionalities occurs. ELS issues in this case are not directly connected to the ISITEP project and to cross-border operations, indeed the same issues can be detected considering a single PPDR communication system operating in a single Country. It is out of the scope of the project to address possible legal and ethical implications due to a misuse of the integrated communication system. However, ISITPE project has to address solutions that prevent a misuse of the system.

A special case of misuse or of use different from intended ones is the "dual use".

Research project outcomes can be subject to dual use issues that is even though they are intended for produce benefits, they might be misapplied causing harmful consequences. For example, new technologies can be potential abused by terrorists or applied for military purposes even if they are originally intended for civil applications.

Even if some Public Safety forces potentially interested in the use of ISITEP framework may be involved in military operations, it has to be highlighted that the use of this tool, allowing PPDR services to roam with their own terminals from one country to another one, is intended for police, civil protection or rescue services and not for direct military aims, where other communication systems are used.

PPDR networks are by their nature secure, reliable and difficult to intercept. These characteristics are in common with military systems, so it could be possible to adapt PPDR communication tools to military applications. Actually, this chance can apply to the use of TETRA or TETRAPOL alone, the presence of an integration framework would just make international and cross-border operations more efficient; for what concern dual use no specific issues can be ascribed to ISITEP.

Functionalities developed in ISITEP are intended to be used just in civil applications, moreover the framework relies on a fixed infrastructure owned and controlled by PPDR agencies and governments. A different use of the framework would be possible only upon approval or violating security restrictions.

In conclusion, even though not all potential eventualities can be foreseen and addressed, it is important to ask if the possibility that the framework can be used from unauthorized people to scopes different from allowed ones is addressed through suitable countermeasures to unwanted access or manipulation.

3.3. PERSONAL DATA PROTECTION AND PRIVACY ASPECTS

ISITEP permits the interoperability among PPDR agencies of federated Countries, allowing migration of PPDR resources and enabling cooperation of operators on the field, and sustains open knowledge on PPDR procedures through specifications and protocols also for future networks. ISITEP, as all the other PPDR related projects, focuses on people safety and protection. As a consequence, the legal, societal and ethical aspects of privacy and data protection assume a relevant role since the framework allows cross-border communications and possible information and data exchange between operators of different countries.

Both privacy and data protection are legal consequences of the political institutionalisation of the private sphere in liberal States, together with the other fundamental human rights. They safeguard the “private sphere” of citizens, acting in different ways: privacy shields the individual while data protection controls entities processing personal data. In general, privacy is not an absolute right, but its interests must be weighed against the interest of preserving the necessary (substantiated) framework functionalities.

The processing of personal data in Europe is regulated by national laws, and guidelines of Directive 95/46/CE. The purpose of the European Directive is to allow the free flow of personal data between Member States, protecting at the same time the fundamental rights and freedoms of persons. The Directive focuses on the right to privacy with respect to the processing of personal data, going further than the protection of the intimacy (generally speaking the private life) with the protection of all the data related to natural persons and not necessarily only the sensitive ones. According to the Directive, the term ‘personal data’ refers to ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is a subject 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.

ISITEP end-users are heterogeneous police forces, rescue teams and first aid operators. Personal data of citizens may be processed, analysed or transmitted to co-operating agencies for sake of security. Therefore, some problems could arise from the new level of police cooperation allowed by ISITEP, because this cooperation is based on information exchange, with violation risks for the fundamental right to privacy. As a consequence, data-treatment becomes an aspect to be addressed within ISITEP project also considering that for safety and emergency issues police and other responders may be covered by laws’ extensions or special rights.

In any case, information collected or exchanged with ISITEP framework shall be used by the competent law enforcement authorities of the Member State to which it has been provided solely for the purposes for which it has been supplied for preventing an immediate and serious threat to public security. Any other processing for different purposes shall be authorized and subject to the national laws of the member states.

ISTEP does not foresee the creation of new databases, but information contained in national repositories may be shared by voice or data message through networks interconnected using ISITEP framework, during cooperation activities. Hence it has to be investigated if ISITEP introduces new issues about privacy and data protection additional to the one already covered by current national laws and international agreements.

Schengen Agreement, for example, enables the creation of a common database, the Schengen Information System (SIS), providing to border officers access to the criminal records of anyone within the contracting State. The SIS is composed of two components: national databases owned by each state (National Schengen Information System, NSIS), and a central database located in Strasbourg, connecting the other and coping and distributing all data. This system has been demonstrated to be very useful in preventing and detecting crimes, but has been also subject to some criticisms for its potential in violating the privacy of the European citizens.

The main privacy protection principle for the SIS is that collected data may only be used for the purposes established for each type of report (see Schengen Art. 39). Moreover, the number of people with access to data is strictly controlled, as well as the accuracy, timeliness, and lawfulness of information entered into the SIS (see Schengen Art 102). Even if direct access to databases of citizens' data is not considered in ISITEP scenarios, the framework allows the access to applications as workflow manager, localization, central address book for dynamic group configuration, and translation systems. In case of remote access to databases through SDS (Short Data Services), it has to be investigated if ISITEP will provide the same security, accuracy, and access control of the SIS, aligning to Schengen articles 39 and 102.

A further concern that has to be taken into account when sharing information is related to that data assume different weight in member state, due to different local laws. An example comes from the restriction of movement freedom within Schengen member states. Citizen right to enter and reside in a Schengen territory depends on domestic laws of each contracting state; if one of them identifies a person as inadmissible under domestic law, this is reported on the NSIS database, automatically copied to the central SIS database and then redistributed to all other national ones. The result is that for a measure placed in act just in one state, the entire Schengen area may become inaccessible to a signalled person. Because information or personal data of citizens are spread through ISITEP framework during cooperation activities, it has to be investigated if these data may assume different weight in various member state, and which are the consequence of their diffusion for involved citizens. It has also to be asked if, when sharing particular data, ISITEP end-users will prevent in some way the possible misalignment of data interpretation under the different national laws.

Special agreements between particular couples of European member states, permanent or active in particular emergency case, may regulate the data exchange between international operators, which may be previously informed and warned about.

It has to be asked if ISITEP protects information exchanged in cross-countries communications in accordance to European Protocol of 8 November 2001 to that Convention, regarding Supervisory Authorities and Transborder Data Flows, and to Recommendation No. R(87) 15 of the Council of Europe, regulating the use of personal data in the police sector. This recommendation establish a set of principles for data protection in activity linked to the finality of "police purposes". The recommendation provides an explicit definition of the expression for "police purposes" that covers "all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order".

The principles of Recommendation R(87)-15 regulate the crucial stages of data protection: collection, storage, use and communication. In the scope of ISITEP this third aspect assumes particular interest, since the framework is not used for data collection or storage, but just for trans-borders communications. This is addressed in section 5.4 of principle 5, describing the situations in which communications of data to foreign police bodies are allowed:

a. *"if there exists a clear legal provision under national or international law,*
b. *in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law, and provided that domestic regulations for the protection of the person are not prejudiced."*

Recommendation R(86)-1 regulates instead the protection of personal data which are indispensable to the effective administration of the social security system, e.g. in co-operation activities between social security institutions (public or private as well) across national borders, including rescue and medical assistance.

The accomplishment by ISITEP framework to these general principles and to the ones outlined in recommendations R(86)-1 and R(87)-15 of the Council of Europe, are further investigated by a set of questions to be applied on ISITEP use case scenarios, collected in section 5.

A specific regime regarding the transfer of personal data to not European countries has been defined by European Union as well, to protect the data subjects whose data are exported outside the territorial scope of the application of the Directive. The scope of ISITEP project is by the way internal to European Union; in case the framework will be exported to be used outside the not-EEA countries, further consideration shall be made.

In the perspective of integrating existing communication systems already used in single countries respecting national laws, the two main ELS aspects arising are related to the security of information exchange and the use of shared data.

3.3.1. SECURITY ASPECTS

Security assumes paramount importance in ISTEP framework, since possible attackers may intercept not only communication regarding citizens' personal data, but also information involving national or international security issues.

ISITEP concerns cooperation and interoperability of PPDR secure networks, which are already used from police and other operators in security or rescue activities (i.e. TETRA and TETRAPOL). These networks implement a strong security level and foreseen various authentication, registration and encryption mechanisms. It has to be investigated if the existing PPDR networks security level is maintained when these are interconnected through ISITEP framework.

For this reason, it has to be verified that ISITEP:

- maintains users registration information and authentication, i.e. the possibility to identify people involved in the communication,
- maintains the encryption to avoid interceptions,
- maintains transmission security to avoid contents alterations or damages.

3.3.2. PERSONAL DATA PROCESSING

The concept of processing concerns any operation performed on personal data, by human or by automatic means. All operation as collection, recording, organization, storage, alteration, retrieval, consultation, disclosure by transmission, dissemination, erasure or destruction of personal data are considered "processing".

More generally, it has to be verified that the use of ISITEP will accomplish the main principles governing the processing of personal data:

- Finality: data must be collected for an explicit, specific, and legitimate purpose.
- Transparency: individuals must be informed of the data collected and of the purpose of collection (with the exception of injured person without consciousness or similar serious cases).
- Legitimacy: processing must be occur for a legitimate reason pursuant to article 7 of European Directive 95/46/CE.
- Proportionality: the personal data collected must be adequate, relevant, and not excessive in relation to the purpose of collection.
- Accuracy and Retention of the Data: individuals' records must be accurate and up to date. False or inaccurate data must be corrected.

All the operations on personal data, collected or analysed within the scope of ISITEP framework, are performed by “processors” under the guideline of a “controller”. European organizations using ISITEP framework (as police, civil protection, rescue services) act as controller when they ask their operators to collect personal data of people during operation on the field. These organizations have the duty of respect European Directive and national laws; it has to be investigated if they will be able to provide the appropriate level of protection on collected/received/processed data.

3.4. ENVIRONMENTAL ISSUES

Environmental impact is no longer a side issue but is central topic also for European Government Policies.
ISITEP framework has therefore to be evaluated also in terms of how they are responsible for protecting and managing the environment in the developing and use of interoperable systems.
Environment is a collective good and its state concerns the entire international community.
Environmental problems affect the health and well-being of very many people, and damage prospects for economic development.
The most common environmental effect of wireless communication systems is the electromagnetic impact.
ISITEP framework shall take into account the recommendations published in 199 by the Council of the European Union (1999/519/EC) on the limitation of exposure of the general public to Electro-Magnetic-Fields (EMF) and the directive of the European Parliament and the Council issued in 2004 (2004/40/EC) on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (EMF). All the national law of states participant to the project shall be respected as well.

Telecommunication systems can by the way also be used for environmental protection and emergencies management, with great benefits. Information and communication technologies can play a vital role in combating environmental problems.
Government and other agencies need to be able to respond rapidly to natural disasters and environmental crises, and an effective cross-border communication system can help them to make the right decisions in time. An effective international PPDR network can give to authorities more time to put in action emergency responses, better management and operational efficiency.

4. APPLICATION OF ELS GUIDELINE FOR ISITEP

This section investigate how the ethical, legal and social guidelines, collected and described in previous chapter, are actually applied to ISITEP outputs, through a list of questions.

The structure follows the major topics of sections 3 focusing on human rights and ethical principles, liability and foreseeable end-use and personal data protection and privacy aspects of ISITEP framework. In particular the provided guidelines of sections 3.2 and 3.3 can be contextualized, by referring to operative scenarios which aim to validate the effectiveness and feasibility of PPDR forces cooperation, through the interconnection of different European networks (see questions in sections 4.2 and 4.3), while the first topic generally refers to ISITEP framework (see questions in section 4.1).

Current version of the deliverable takes into account the ELS analysis applied to Scenario 1 (WP 7.1), for Norwey-Sweden (NO-SE) trial. Other scenarios will be taken into account in the next version of the document.

Scenario 1 (WP 7.1) is a showcase of the interconnection of the two live TETRA networks in Norway (Nødnett) and in Sweden (Rakel). This will involve connecting the two TETRA networks over an ISI E1 gateway (D4.7.1), use radio terminals with ISI software, control rooms as well as utilizing products from the ISITEP framework such as legal agreements, functional model and handbook on PPDR procedures (SP 3 deliverables). The information that are being shared in this set-up and scenario is voice over TETRA and SDS messages.

The Norway-Sweden trial (WP71) will be a full scale cross-border field exercise where the technology as well as procedures for a joint operation between public safety agencies from the two countries will be played out utilizing the ISITEP framework (See D71.1 for more information on the scenario and utilized technologies). The NO-SE scenario in itself is an incident where a bus with many passengers has been pushed off the road and overturned on the Norwegian side of the border but close to Sweden. It is later discovered that the car which caused the bus accident is wrecked on the Swedish side of the border and the drivers have escaped from the scene – initiating a search and rescue mission. Swedish resources are asked to respond across the border to assist in the rescue of passengers, traffic control and to limit material damage. Both Norwegian and Swedish resources from police, fire/rescue, health/ambulance, supported by the control room operators will participate and receive assistance from resources from the neighbouring country. Various teams are assigned international agency specific and/or international multi-agency talk groups (WP3.2 deliverable).

4.1. VERIFICATION OF HUMAN RIGHTS AND ETHICAL GUIDELINES APPLICATION

Following questions aim to generally verify the application of human rights and ethical guidelines of ISITEP project to the deriving framework.

1. **Why are ISITEP outputs useful in a democratic society?**

   ISITEP responds to the European recommendation in terms of international cooperation, proposing advanced solutions to satisfy communications needs of PPDR organizations in cross-border communications.
   The European Council "Recommendation on improving radio communication between operational units in border areas" of 2009 highlighted the importance of the interoperability between PPDR organizations in border areas: "effective cross-border cooperation requires adequate communication capabilities including interoperable radio communication systems in border areas and between operational services from different Member States".

Past programs such as the Stockholm Programme "An open and secure Europe serving and protecting the citizen", were used by European Union to promote more close cooperation of European countries in border management and disaster relief:
"An internal security strategy should be developed in order to further improve security in the Union and thus protect the lives and safety of European citizens and tackle organised crime, terrorism and other threats. The strategy should be aimed at strengthening cooperation in law enforcement, border management, civil protection, disaster management as well as criminal judicial cooperation in order to make Europe more secure."
The framework is intended to increases citizens' security by enabling the coordinated management of police and rescue activities in cross border and other international cooperation.

2. **Is ISITEP project able to reach its goal in conformity with proportionality and subsidiarity principles? Is the relation between the used means and foreseen goal well defined?**

   Means are proportionated to project development since it takes advantage of communication infrastructures which are already present. The development of ISITEP framework has not a deep impact on society and economy since its functionalities are already available in each involved state and technology, but they are made more efficient for cross border operations. ISI also provides the ability to move (migrate) with the radio terminal from the home network to be used in another network.

3. **Are the goals and the improvements of ISITEP project well defined and documented?**

   Goals are described in the "DoW" document and in D1.1 "Detailed implementation plan" document; all project outputs are included in project deliverables. All this information are promoted trough dissemination activities.

4. **Are the purposes, scopes and functionalities of the project available to the public at large?**
   The project outputs are oriented to define a framework that is not directly used by citizens but it is addressed to a restricted users' community. Although the public at large is not aware of or interested in technological details, it is important to clarify the relevance of an efficient cooperation in transnational operations. This can be done by means of proper dissemination activities.

5. **Are the interim and final achievements documented and made available to the public?**
   General ethical and legal constraints should to be explained both to supervising authorities and public. Complete transparency is achieved disseminating project related news and facts on different types of publications. Website is the main means of communication that permit to describe what is done. Between others, it permit to make available (in public or restricted areas, depending on the publishing policies) project deliverables that contain information about purposes and results. Other media like social networks (e.g. Facebook, Twitter, LinkedIn, YouTube, etc.) should be used both to inform and to have a return channel to obtain feedback from both stakeholders and citizens. They can follow step by step the done work and can verify that the financial commitment is justified from both foreseen and obtained objectives related to social advantages that come from increase the efficiency and security of PPDR activities and participate to scientific and technological evolution.
   This policy does not assure that all citizens read this information, but their public availability and possibility to be reached throw search engines are an effective mean to inform public.

6. **Are also aspects related to the end use of ISITEP been taken into account?**

Beside dissemination activities, a suitable information campaign should be performed by European countries that will adopt the ISITEP framework to both inform the citizens of new tools available for society security improvement but also to make aware them of possibility to deal with synergic forces equipped with advanced and structured communication tools.

4.2. VERIFICATION OF LIABILITY AND FORESEEABLE END-USE GUIDELINES APPLICATION: QUESTIONS

Following questions aim to verify the application of liability and foreseeable end-use guidelines of ISITEP framework; the answers will be provided in following subsections, considering the context of the specific application scenarios of the demos.

7. **What is the approach of the framework to legal requirements, mainly referred to the fact that multiple national legislation are involved and they can slightly differ each other?**

8. **What is the approach to assess that the framework is legal in each state it could be used?**

9. **After the interconnection of the international networks, thanks to ISI functionality and the outputs form ISITEP project, is the resulting communication system properly protected from use by unauthorized people that can exploit it for unwanted purposes (e.g. terrorists, hackers or soldiers)? In particular is the protection against unauthorized access of TETRA and TETRAPOL guaranteed when they are interconnected?**

10. **Are the local "responsible bodies" (authority, service or other public body) which are competent under national laws, well identified for each participant country?**

4.2.1. VERIFICATION OF LIABILITY AND FORESEEABLE END-USE GUIDELINES APPLICATION: ANSERWES FOR SCENARIO 1

Here following the answers related to Scenario 1.

7. **What is the approach of the framework to legal requirements, mainly referred to the fact that multiple national legislation are involved and they can slightly differ each other?**
There are at least two levels of legal requirements to be considered for the NO-SE case. One is the network infrastructure level concerning network security, available frequencies and other regulations, which are handled by the national network operator/owner. MSB and DNK are the responsible agencies regulating these networks and a legal agreement between MSB/DNK is necessary to perform the NO-SE scenario. This agreement is currently under development and the end-product will be documented in a WP3.1 deliverable.

   The other level concerns the end-user organisations, the legal requirements related to the use of the ISI functionality and the legal agreements to professionally operate in another country. In particular for the NO-SE scenario police, health and fire and emergency services from both Norway and Sweden will participate. For operations such as the bus accident there is an existing collaboration between these agencies in Norway and Sweden based on legal agreement called NORDRED. Thus, a major *advantage of connecting the networks between Norway and Sweden is the long term collaboration between the end-users and legal agreements between the states. Procedures for cross-border collaboration is a WP3.3 deliverable.*

8. **What is the approach to assess that the framework is legal in each state it could be used?**
   This question is related to regulations of the national network and the legal agreements among network owners on a state level, to allow foreign network users access and to grant user rights to the national network (the first level in the previous question). In particular for the NO-SE scenario the legal agreement between Norway and Sweden (under development in WP3.1) is being assessed by lawyers in MSB and DNK to ensure that the framework is applicable in each state. The lawyers have mapped the key topics to this agreement (i.e. access and user rights, responsibility for transmission between the two networks, service agreements, cost allocation, confidentiality etc). This agreement is a fundamental basis for the NO-SE scenario since the interconnection between the networks cannot happen before an agreement is in place.

9. **After the interconnection of the international networks, thanks to ISI functionality and the outputs form ISITEP project, is the resulting communication system properly protected from use by unauthorized people that can exploit it for unwanted purposes (e.g. terrorists, hackers or soldiers)? In particular is the protection against unauthorized access of TETRA and TETRAPOL guaranteed when they are interconnected?**
   This is an important question when connecting two national PPDR networks. ISI is a functionality within and between national PPDR networks. Security issues are thus regulated for each national network, and in agreements between national network owners. For the NO-SE scenario both Nødnett and Rakel have security class 3 and is protected from unauthorized use. The challenges arise because of the transmission between these two networks. In the NO-SE scenario dedicated transmission lines (E1 over IP) will be used over the STESTA (Secure Trans European Services for Telematics between Administrations) [4] network to ensure that this connection is protected.

10. **Are the local "responsible bodies" (authority, service or other public body) which are competent under national laws, well identified for each participant country?**
    Local "responsible bodies" are primarily the PPDR network owners in each country, which in the NO SE scenario are MSB (Sweden) and DNK (Norway). In addition police, health, fire & rescue services, SOS Alarm (control room owner in Sweden) and representatives from the local municipalities are participants in the scenario. Some of these actors will use the ISI ready radio terminals (which are being developed outside the ISITEP scope) and use elements from the ISITEP framework, while others are supporting bodies in the scenario. Thus, the relevant responsible bodies are identified for the NO-SE scenario.

4.3. VERIFICATION OF PERSONAL DATA PROTECTION AND PRIVACY ASPECTS GUIDELINES APPLICATION

Following questions aim to verify the application of personal data protection and privacy guidelines of ISITEP framework; the answers will be provided in following subsections, considering the context of the specific application scenarios of the demos.

11. **Have the possible consequences of the heterogeneous composition of talking groups (police and civil forces) been take into account?**

12. **Are the information (voice calls, SDS etc.) passing through the integrated communication system protected from interception? In particular, is the protection level against interception of TETRA and TETRAPOL guaranteed within the integrated framework?**

13. **Can information pass through not secure links or network equipment (e.g. satellite, shared links, commercial operators' networks, etc.)?**

14. **In case some personal data (of citizens or PPDR users) or sensitive information are exchanged (trough voice conversation, SDS or other communication services), are these only automated, or also manual processed? In case, are some procedures foreseen to verify that the aim of manual processing is clear and authorized?**

15. **Are some procedures foreseen with the aim to verify that in some of the involved countries is there any authority empowered to authorise the police authorities to communicate personal data (of citizens or PPDR users) collected during the operations to other public bodies?**

16. **Are some procedures foreseen with the aim to verify that in some of the involved countries is there any authority empowered to authorise the police authorities to communicate personal data (of citizens or PPDR users) collected during the operations to any private party?**

17. **In trans-national multi-agency operations, are the talking group participants aware of other participants and of possible restrictions to information that can be shared? For example, can the criminal records be freely communicated to civil operators?**

18. **Are some procedures foreseen with the aim to verify that the police authorities have a "legitimate interest" in obtaining sensitive information or personal data (of citizens or PPDR users) in communications between other countries?**

19. **Have possible differences in sensible information or personal data definition and treatment (e.g. privacy lows) between different states been investigated and faced?**

20. **Are sensible information or personal data (of citizens or of PPDR users) shared during cooperation activities permanently stored by one of the participant countries for administrative purposes?**

21. **Are the accuracy and the quality of exchanged information been verified before communicated to other countries authorities? Are there any case where incomplete or not up to date data may be anyway shared?**

22. **Are the request to access data in some way registered? Are some communication logs collected?**

23. **Are sensible information or personal data (of citizens or of PPDR users) kept for police purposes deleted if they are no longer necessary for the purposes for which they were stored?**

4.3.1. VERIFICATION OF PERSONAL DATA PROTECTION AND PRIVACY ASPECTS GUIDELINES APPLICATION: ANSERWES FOR SCENARIO 1

Here following the answers related to Scenario 1.

11. **Have the possible consequences of the heterogeneous composition of talking groups (police and civil forces) been take into account?**
    Yes, the structure of and access to international talk groups will be regulated by the network or talk group owner(s). For example in the NO SE scenario (bus accident) the use of talkgroups will be regulated by a functional model agreed upon by the different agencies (this will be covered WP3.2). For example: the police forces will have pre-defined and dedicated talk groups where other agencies are prohibited (both by configuration in terminals and methodology) and only police agencies can listen to them.

    Other cross-agency talk groups (NO-SE EM / NO-SE CO talk groups) are available for other groups of agencies and must be considered heterogeneous. In the EM groups the emergency agencies (police, health and fire services) can communicate together. In the CO groups all collaborating parties can communicate. This way information sharing can be adjusted to which talk group they are talking in. The emergency agency end-users have developed the rules for these groups. The project group are also planning education and training courses for the participants in the NO-SE scenario (demo) to ensure that heterogeneous talk groups are used in accordance with agreed upon guidelines.

12. **Are the information (voice calls, SDS etc.) passing through the integrated communication system protected from interception? In particular, is the protection level against interception of TETRA and TETRAPOL guaranteed within the integrated framework?**

    Yes, there are some issues that must be handled when connecting to networks. As explained in question 9 the interconnection is the vulnerable element. Specific for the NO-SE scenario this will be secured by an STESTA connection between the gateways.

    E2E encryption is not guaranteed by default when connecting two live networks. Specific to the NO-SE scenario E2E encryption is ensured in Nødnett and in Rakel in their respective KMF (Key Management Facility). When connecting the two networks some issues are yet to be solved to ensure that linked talk groups and migrated radios establish the E2EE encryption. One way to solve this is to ensure that relevant Swedish terminals and talk groups are provisioned in the other countries KMF. DNK/MSB is in dialogue with the police agencies to find a solution to this.

13. **Can information pass through not secure links or network equipment (e.g. satellite, shared links, commercial operators' networks, etc.)?**

    See 9 and 10. For the NO-SE scenario, all voice and SDS data passes through the dedicated networks in Norway and Sweden. Between Norway and Sweden information will pass through secure transmission lines between the ISI gateways in the respective countries. These lines will still be E1 over IP – so to ensure proper protection DNK/MSB will ensure that this will go over STESTA. Please confer with SP4 deliverables for more information on transmission between gateways.

14. **In case some personal data (of citizens or PPDR users) or sensitive information are exchanged (trough voice conversation, SDS or other communication services), are these only automated, or also manual processed? In case, are some procedures foreseen to verify that the aim of manual processing is clear and authorized?**

    No personal data of citizens is processed through NO-SE ISI and personal data of injured persons are handled by health professionals only. For what concerns personal data of the PPDR users, in Norway the identification numbers of the radio terminals (ISSI numbers) are regarded as personal data and they can be tracked to specific PPDR users. Norway has therefore ensured that these numbers are removed when storing traffic data (meta data such as number of calls on a basestation, conversation length, used talk groups, etc). The lawyers in Norway and Sweden are currently looking for possible differences iin practice in the two countries and how this sensitive information can be treated. Processing is a local control room task.

15. **Are some procedures foreseen with the aim to verify that in some of the involved countries is there any authority empowered to authorise the police authorities to communicate personal data (of citizens or PPDR users) collected during the operations to other public bodies?**
    This is not applicable to the NO-SE scenario. No authority will inform the police to communicate personal data collected during the bus accident scenario.

16. **Are some procedures foreseen with the aim to verify that in some of the involved countries is there any authority empowered to authorise the police authorities to communicate personal data (of citizens or PPDR users) collected during the operations to any private party?**
    N/A. In the NO-SE scenario personal data is not shared with any private party. No private security agency or other third party have access to the national PPDR networks.

17. **In trans-national multi-agency operations, are the talking group participants aware of other participants and of possible restrictions to information that can be shared? For example, can the criminal records be freely communicated to civil operators?**
    This is regulated in agreements and legal framework between the respective countries. Also (as explained in question 11) there is a clear functional model for the NO-SE scenario, in addition to guidelines developed by the end users to avoid this. For example, the police will have talk groups that only police officers can join, health services will have talk groups only health personnel can join and the same for firefighting forces. These are the default talk groups the participants will use. They will

also use "emergency" and "cooperation" talk groups where participants from other agencies can hear them – but they will be aware of that since they must change talk groups manually. Also, this is the same way Norwegian and Swedish end-users work today in their own countries and is not unique for the ISITEP framework. What is *unique for the ISITEP framework is the awareness that users from the same agency – but different country – can listen to the NO-SE talk groups.*

18. **Are some procedures foreseen with the aim to verify that the police authorities have a "legitimate interest" in obtaining sensitive information or personal data (of citizens or PPDR users) in communications between other countries?**
    This is regulated in international agreements for cooperation among forces.

19. **Have possible differences in sensible information or personal data definition and treatment (e.g. privacy lows) between different states been investigated and faced?**
    These issues are being identified and solved by the MSB/DNK lawyers in the legal agreement under development in SP 3 (see also previous answers). The two most pressing themes are storing of ISSI numbers and voice logs.

20. **Are sensible information or personal data (of citizens or of PPDR users) shared during cooperation activities permanently stored by one of the participant countries for administrative purposes?**
    This kind of activities regards local/national control rooms; this issue can be part of the legal agreement in WP3.1.

21. **Are the accuracy and the quality of exchanged information been verified before communicated to other countries authorities? Are there any case where incomplete or not up to date data may be anyway shared?**
    In general, information exchanged are reliable. Some exception can occur in emergency situation when the priority is the promptness of the communication and up to date data are not available.

22. **Are the request to access data in some way registered? Are some communication logs collected?**
    All call data records from use of resources in any national networks are stored. Handling of these are regulated nationally and will be subject for legal agreement between the national network owners/operators.
    Communication logging activity is regulated in international agreements for cooperation among forces. In the considered scenario, control rooms in Norway store voice records of the conversations in talk groups. These issues are being studied in WP3.1, in the legal agreement between Norway and Sweden. The two countries may e.g. have different regulations regarding storing of voice logs. These issues are currently under study.

23. **Are sensible information or personal data (of citizens or of PPDR users) kept for police purposes deleted if they are no longer necessary for the purposes for which they were stored?**
    This is regulated by policies of local/national control room and is not part of the ISITEP framework.

5. GENERAL CONSIDERATION ON ELS IN ISITEP PROJECT DEVELOPMENT

ISITEP activities are intended to achieve new and better results to improve disaster recovery and security against crimes, with societal conditions improvement.

Three major aspects affect ELS consideration to be done in ISITEP project development:

- *the nature of the projects partners;*
- *the project partners nationality;*
- *the existence of mission statements and code of ethics in each industry/organization/research organization.*

To make ISITEP as conform as possible to proportionality and substantiality principles, already described in section 3, also for what concerns the project development, its purposes should be made public and promulgated pursuing an approach of full transparency to the public. This can be achieved, for example, through:

- making clear the reasons for existence of the project, substantiating why it is important to develop the ISITEP framework;
- clearly specifying its purposes;
- substantiating compliance with ethical and legal requirements by incorporating technical and organizational safeguards in view of:
  - functions and outcomes misuse of the ISITEP researches (restricted access, authorization, login of use etc.);
  - legitimate data processing (anonymization, encryption, security etc.);
  - legitimate eventual use of materials protected by intellectual property rights obtaining a license from rights owner.
- Continuously monitoring and disseminating activities status and reached goals.

Analysing the nature of the project partners we can observe that it is composed mainly by high technological enterprises and end users (first responders). In particular, the project involves personnel expert of technological aspects. In this context it is possible to have gender inequalities that, in general, don't derive from the used technology or project results, but instead come from a cultural trend that sees men more interested in engineering related arguments than women.

An important aspect to be underlined is that the partners involved in the project and other stakeholders are European, therefore they are subject to communitarian legislation. This assures a uniformity of regulation that reduces at minimum possible incongruences and legislative gaps among the partners. Indeed, since the project deals with national security, public safety, crimes and disaster prevention and management, going further single national frontiers, special attention has to be paid to legal issues that can result from national and/or community law violation.

In particular laws on the protection of individuals, work and privacy concern with the project.

Finally, another important item in a technical research project to be taken into account is the Intellectual Property Rights (IPR) protection. In this sense the partners have signed a Consortium Agreement to define the main rules and policies for publications and property of the project results.

5.1. RESPECT FOR INDIVIDUALS

Respect for individual is a universally recognised principle ratified in the Universal Declaration of Human Rights. Also in research activities, the respect for human dignity shall to be considered as fundamental, avoiding all possible actions that imply or can cause voluntarily or not, physical or moral damages or sufferance. Ethic issue can arise if research activities involves children, incapable people, human genetic or biological material, personal sensible data, experiments on animals, etc. Under the principle of equality, any kind of gender/religion/cultural/lingual discrimination have to be refused.

European Commission encourages the addressing of gender issues in research, designing and implementing equal opportunity policies intended to achieve a gender balance in the workforce and promoting the involvement of women in research playing the role both of scientist and manager.

Subjects involved in the project shall be informed about its purposes and consequences. They shall to know who is funding the project to avoid pressures and that their participation in the project is voluntary and can be refused in case of legitimate concerns.

Worker have to be provided with a sustainable and healthy environment and with all tools necessary to perform foreseen activities. Aspirations and inclinations of individual shall be respected. Cooperation shall be promoted in order to increase sustainability and value people and their work and enhance their professional capabilities and at the same time contribute to obtain an added value for project objectives achievement.

To act in an ethical and professional manner should became a clear and conscious choice for people that have to be encouraged to share and promote it with others.

5.2. PRIVACY AND DATA PROTECTION

Personal data confidentiality is a right for all people. Even in research activities, security and privacy of citizens and worker have to be protected.

If during the project development personal data are collected, managed or stored, the right to privacy shall to be respected permitting the access, verification, modification and erasing of information and maintaining confidentiality. Re-use of personal data is not permitted without consent.

5.3. INFORMATION EXCHANGE

Information exchange shall to occur on a fair, honest, secure, complete and accurate manner.

All the documents related to the project must be treated following specific procedure of security classification and exchange. This topic is detailed addressed in Task 85.2.

5.4. SUSTAINABILITY

Electromagnetic issues is maybe the most evident environmental impact of ISITEP framework and its effect have to be taken into account, as reported in section 3.4. It is anyway important that project partners maintain an eco-friendly behaviour during the project development; it is in facts nowadays clear that almost all the humans' activities imply environmental impacts. Project partners are therefore encouraged to maintain a responsible behaviour in the everyday activities related to the project development, e.g. limiting the energy consumptions, reducing the number of printed documents, avoiding de-visu international encounters when is possible to substitute them with digital meetings, etc…

5.1. INTELLECTUAL PROPERTY

Intellectual Property Rights (IPRs) define the value to be given to mind creations. Intermediate results and final outcomes of a research project have an indisputable societal as well as economic value that shall to be protected. The rules that apply to ISITEP foreground are stated in consortium agreement. In particular property of foreground generated from single or several parties is established, together with resources access policies. From an ethical point of view, these principles should to be respected especially in dissemination or publication activities of either part or whole project outcomes.

ISITEP framework development is conducted by a consortium, however in carrying activities out it could became necessary to resort to third part resources, either hardware or software.

For what concerns software or editorial products, they can be available from open or restricted access sources. In the first case, the resource is freely available (e.g. from Internet, magazines, etc.), without access restriction or payment requirements. The free access, however, does not imply they are not subject to property rights. Many texts or images available on the Internet are copyrighted, which implies that they cannot freely be copied, adapted, or distributed. The missing of a copyright notice, the lack of technical protection means or of an indication of rights holder that he retains, exercises or enforces his right, is not sufficient to retain the resource usable. Protected works can only be copied or made available to the public with a license from the rights holder or where an exception to an exclusive right is applicable.

The legislation in the field of intellectual properties is not uniform between European Member States. The law applicable to infringement of IPR is the law of the country in which the rights holder seeks to have his rights protected.

6. PROCEDURES FOR ELS ASSESSMENT DURING ISITEP PROJECT DEVELOPMENT

One of the goals of work package WP85 is to define and actualize a common view within the project partners about ethical, legal and societal (ELS) issue involved in the framework. All topics and procedures shall be harmonised, agreed and realisable during the execution of ISITEP project.

ELS aspects arise in both the project research topics and in the way they are developed from stakeholders.

The analysis provided in this work package helps in understanding how these issues may impact on the organization of ISITEP.

The management of ELS by project partners during the project lifecycle will be traced in two documents that will be delivered: the “Detailed report on the ethical, legal and societal aspects of the project”, freezing status of ELS within the project at the end of the first working year, and the “Final report on the ethical, legal and societal aspects of the project” at the conclusion of the project.

Deliverable Number	Deliverable Title	Nature	Dissemination Level	Delivery Date
D85.1	Detailed report on the ethical, legal and societal aspects of the project	R	PU	T0 + 12
D85.4	Final report on the ethical, legal and societal aspects of the project	R	PU	T0 + 36

Table 1: the two ELS deliverable will be provided respectively after the first working year and at the end of the project.

Taking into account ISITEP specific characteristics analysed before, the ELS topics relevant for the project can be identified in:

- *workforce Statistics.*
- *management of the project,*
- *innovation of the project and resources’ use,*
- *communication between partners,*
- *documents treatment,*
- *company Ethic code,*
- *environmental issues.*

To investigate and address these topics an ELS report called “*Survey on ethical, legal and societal aspects*”, is here defined and distributed among the partners. The goal is to check the satisfaction of the ELS principles defined here.

The survey wants to maintain the transparency toward other project partners, and eventually adjust the steps needed to reach solid long-term foundation of ISITEP in ethical, legal and social aspects.

The reports are collected by the Task leader, following the standard procedure for collecting documental contributions, and integrated in the D85.1 report.

In particular this analysis will be performed twice, one at the end of the first year and the other at the end of the project.

The first ELS surveys filled out by all partners, are reported in this deliverable with the purpose of share their approach to ethical, legal and societal and the strategies followed to cope these aspects.

In particular this first view helps identifying possible discrepancies in the ELS management of partners, and use this feedback to take internal actions in project development to fix possible problems.

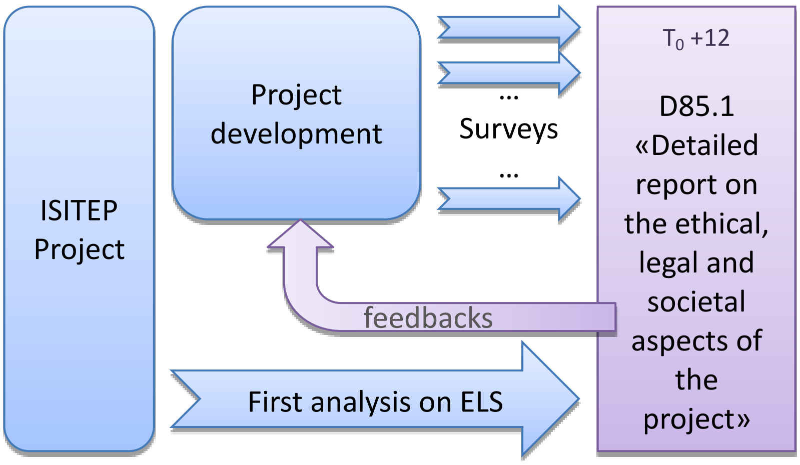
ISITEP Project
Project development
…
Surveys
…
T_0 +12
D85.1 «Detailed report on the ethical, legal and societal aspects of the project»
feedbacks
First analysis on ELS

Figure 1: The first report will be provided at T_0+12 and used for possible feedback and adjustment in project developing procedures

The second surveys will be provided at the end of the activities, reporting the overall broad picture of ELS implication of ISITEP project and of the way it has been developed, resulting by all the performed activities and by the complete analysis of deliverables, background papers, proposals for approaches and methodologies followed in the project.

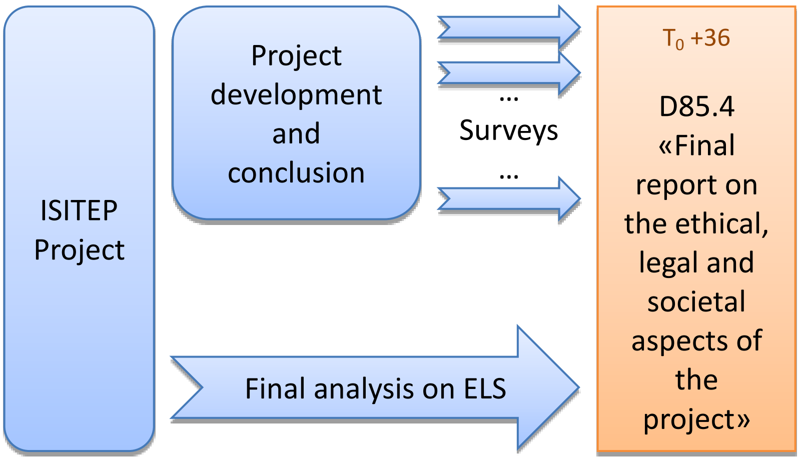
ISITEP Project
Project development and conclusion
…
Surveys
…
T_0 +36
D85.4 «Final report on the ethical, legal and societal aspects of the project»
Final analysis on ELS

Figure 2: The final report will be provided at T_0+36, with the cumulative view of ELS issues involved in the project and their management

Following two sections report respectively the template to be used to collect project partners' surveys and the summarized obtained results. The complete collection of surveys filled by partners can be found in Appendix A.

6.1. “SURVEY ON ETHICAL, LEGAL AND SOCIETAL ASPECTS OF THE PROJECT” TEMPLATE

1. PARTNER NAME:

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, …

Type of Position	**Number of Women**	**Number of Men**
Scientific Coordinator		
Work package leaders		
Experienced researchers (i.e. PhD holders)		
PhD Students		
Other		

How many additional researchers (in companies and universities) were employed specifically for this project?	YES / NO
Of which, indicate the number of women:	…
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES / NO
Did your company carry out specific Gender Equality Actions under the project?	YES / NO
Did your company respect the privacy of employees, correctly treating workers personal data?	YES / NO

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES / NO
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES / NO
Did you notice any actions or circumstances that could be construed as a conflict of interest?	YES / NO
In this case, did you report them to the project partners and other stakeholders?	YES / NO / NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behaviour between internal and shared working teams?	YES / NO

C. IPR

Did your company respect and protect intellectual property rights of others?	YES / NO

Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES / NO
D. Communication between partners	
There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES / NO
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES / NO
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES / NO
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? …………………………………………………… ……………………………………………………	
E. Documents treatment	
Are all project documents treated as requested by correspondent security classification and security needs?	YES / NO
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES / NO
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES / NO
F. Company Ethic code	
Does it exist in your company activity a common mission statement or a company code of ethic?	YES / NO
In this case are these respected by this project?	YES / NO
Is the professional deontology applied in the project development?	YES / NO
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? …………………………………………………… ……………………………………………………	
Did you analyse the ethic's code of the partner companies, checking if it respect the one of your company?	**YES / NO**
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES / NO
In case an ethic issue have no correspondence on laws or European recommendation,	

how will you act? ………………………………………………… …………………………………………………	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	YES / NO
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES / NO
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES / NO

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	YES / NO
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	YES / NO

6.2. GLOBAL RESULTS ON "SURVEY ON ETHICAL, LEGAL AND SOCIETAL ASPECTS OF THE PROJECT"

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	75% Men 25% Women

Type of Position	**Women**	**Men**
Scientific Coordinator		4,7%
Work package leaders	3,1%	14%
Experienced researchers (i.e. PhD holders)	9,5%	18,7%
PhD Students		
Other	12,5%	37,5%

How many additional researchers (in companies and universities) were employed specifically for this project?	5,8% of total workers
Of which, indicate the number of women:	75%
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES 100%
Did your company carry out specific Gender Equality Actions under the project?	YES 50% NO 50%
Did your company respect the privacy of employees, correctly treating workers	YES 100%

personal data?	

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES 100%
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES 100%
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO 100%
In this case, did you report them to the project partners and other stakeholders?	NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behaviour between internal and shared working teams?	YES 87.5% N.A. 12.5%

C. IPR

Did your company respect and protect intellectual property rights of others?	YES 100%
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES 100%

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES 100%
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES 100%
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES 100%
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies?	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES 100%
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES 100%
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES 100%

F. Company Ethic code	
Does it exist in your company activity a common mission statement or a company code of ethic?	YES 87,5% NO 12,5%
In this case are these respected by this project?	YES 87,5% N.A. 12,5%
Is the professional deontology applied in the project development?	YES 87,5% N.A. 12,5%
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines?	
Did you analyse the ethic's code of the partner companies, checking if it respect the one of your company?	YES 50% NO 50%
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES 75% NO 25%
In case an ethic issue have no correspondence on laws or European recommendation, how will you act?	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	YES 100%
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES 75% NO 12,5% N.A. 12,5%
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES 100%
G. Environmental issues	
Are you taking into account the environment respect and possible environment impact of the project?	YES 87,5% NO 12,5%
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	YES 12,5% NO 75% N.A. 12,5%

These results will be shared and discussed with consortium partners and the will be update during upcoming year, according the procedure described in previous section.

7. BIBLIOGRAPHY

[1] Commission of the European Community – "COMMUNICATION FROM THE COMMISSION on the precautionary principle" - Brussels, 02.02.2000

[2] http://www.virtuoso.eu/

[3] http://www.indect-project.eu/

[4] STESTA: Secure Trans European Services for Telematics between Administrations

APPENDIX A - PARTNERS SURVEYS

ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, 5

Type of Position	**Number of Women**	**Number of Men**
Scientific Coordinator		1
Work package leaders		4
Experienced researchers (i.e. PhD holders)		
PhD Students		
Other		

How many additional researchers (in companies and universities) were employed specifically for this project?	1
Of which, indicate the number of women:	1
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES
Did your company carry out specific Gender Equality Actions under the project?	YES
Did your company respect the privacy of employees, correctly treating workers personal data?	YES

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO
In this case, did you report them to the project partners and other stakeholders?	NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behaviour between internal and shared working teams?	YES

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and	YES

research contributions employees and of others?	
D. Communication between partners	
There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? NOT Applicable	
E. Documents treatment	
Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES
F. Company Ethic code	
Does it exist in your company activity a common mission statement or a company code of ethic?	YES
In this case are these respected by this project?	YES
Is the professional deontology applied in the project development?	YES
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? Laws & Rules by Italian Government	
Did you analyse the ethic's code of the partner companies, checking if it respect the one of your company?	NO
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES
In case an ethic issue have no correspondence on laws or European recommendation, how will you act? ………………………………………………..	

……………………………………………….	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	YES
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	YES
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	YES

CASSIDIAN FINLAND OY

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, 6

Type of Position	Number of Women	Number of Men
Scientific Coordinator		1
Work package leaders		1
Experienced researchers (i.e. PhD holders)	1	1
PhD Students		
Other		2

How many additional researchers (in companies and universities) were employed specifically for this project?	0
Of which, indicate the number of women:	…
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES
Did your company carry out specific Gender Equality Actions under the project?	NO
Did your company respect the privacy of employees, correctly treating workers personal data?	YES

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO
In this case, did you report them to the project partners and other stakeholders?	YES / NO / NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behaviour between internal and shared working teams?	YES

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? ………………………………………………. ……………………………………………….	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES

F. Company Ethic code

Does it exist in your company activity a common mission statement or a company code of ethic?	YES
In this case are these respected by this project?	YES
Is the professional deontology applied in the project development?	?
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? ………………………………………………. ……………………………………………….	
Did you analyse the ethic's code of the partner companies, checking if it respect the one of your company?	NO
Did your company consider the possible conflicts in international norms and laws involved in the project?	NO
In case an ethic issue have no correspondence on laws or European recommendation, how will you act? ……………………………………………….	

……………………………………………….	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	YES
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	YES
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	NO

UNIVERSITAT POLITECNICA DE CATALUNYA

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, ...3

Type of Position	**Number of Women**	**Number of Men**
Scientific Coordinator	0	0
Work package leaders	0	0
Experienced researchers (i.e. PhD holders)	0	3
PhD Students	0	0
Other	0	0

How many additional researchers (in companies and universities) were employed specifically for this project?	NO
Of which, indicate the number of women:	NOT APPLICABLE
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES
Did your company carry out specific Gender Equality Actions under the project?	YES
Did your company respect the privacy of employees, correctly treating workers personal data?	YES

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO
In this case, did you report them to the project partners and other stakeholders?	NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behavior between internal and shared working teams?	YES

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? …………………………………………………. ………………………………………………….	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES

F. Company Ethic code

Does it exist in your company activity a common mission statement or a company code of ethic?	YES
In this case are these respected by this project?	YES
Is the professional deontology applied in the project development?	YES
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? …………………………………………………. ………………………………………………….	
Did you analyze the ethic's code of the partner companies, checking if it respect the one of your company?	YES
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES
In case an ethic issue have no correspondence on laws or European recommendation, how will you act? ………………………………………………….	

…………………………………………………..	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	YES
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	YES
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	NO

MOTOROLA SOLUTIONS DANMARK AS

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, 9

Type of Position	Number of Women	Number of Men
Scientific Coordinator	0	0
Work package leaders	0	1
Experienced researchers (i.e. PhD holders)	1	3
PhD Students	0	0
Other	1	3

How many additional researchers (in companies and universities) were employed specifically for this project?	2
Of which, indicate the number of women:	1
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	Yes
Did your company carry out specific Gender Equality Actions under the project?	Yes
Did your company respect the privacy of employees, correctly treating workers personal data?	Yes

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	Yes
Did your company encourage team members to conform to the standard of conduct expected for the project?	Yes
Did you notice any actions or circumstances that could be construed as a conflict of interest?	No
In this case, did you report them to the project partners and other stakeholders?	NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behavior between internal and shared working teams?	YES

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? Not applicable	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES

F. Company Ethic code

Does it exist in your company activity a common mission statement or a company code of ethic?	YES
In this case are these respected by this project?	YES
Is the professional deontology applied in the project development?	YES
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? Yes	
Did you analyze the ethic's code of the partner companies, checking if it respect the one of your company?	YES
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES
In case an ethic issue have no correspondence on laws or European recommendation, how will you act? According to existing company policy: "Code of Conduct"	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and	YES

cultural differences?	
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	YES
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	Not applicable during 1st year

NET TECHNOLOGIES ETAIREIA PERIORISMENIS EFTHYNIS

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:		Total, 5.
Type of Position	**Number of Women**	**Number of Men**
Scientific Coordinator		
Work package leaders		1
Experienced researchers (i.e. PhD holders)	1	3
PhD Students		
Other		
How many additional researchers (in companies and universities) were employed specifically for this project?		NO
Of which, indicate the number of women:		…
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?		YES
Did your company carry out specific Gender Equality Actions under the project?		NO
Did your company respect the privacy of employees, correctly treating workers personal data?		YES

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO
In this case, did you report them to the project partners and other stakeholders?	NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behavior between internal and shared working teams?	

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? …………………………………………………. ………………………………………………….	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES

F. Company Ethic code

Does it exist in your company activity a common mission statement or a company code of ethic?	YES
In this case are these respected by this project?	YES
Is the professional deontology applied in the project development?	YES
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? …………………………………………………. ………………………………………………….	
Did you analyze the ethic's code of the partner companies, checking if it respect the one of your company?	NO
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES
In case an ethic issue have no correspondence on laws or European recommendation, how will you act? ………………………………………………….	

………………………………………………..	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	YES
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	YES
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	NO

Norway DNK

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, 19

Type of Position	Number of Women	Number of Men
Scientific Coordinator		
Work package leaders	1	0
Experienced researchers (i.e. PhD holders)	1	0
PhD Students		
Other	3	14

How many additional researchers (in companies and universities) were employed specifically for this project?	NO
Of which, indicate the number of women:	…
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES
Did your company carry out specific Gender Equality Actions under the project?	NO
Did your company respect the privacy of employees, correctly treating workers personal data?	YES

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO
In this case, did you report them to the project partners and other stakeholders?	NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behavior between internal and shared working teams?	YES

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? …………………………………………………. ………………………………………………….	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES

F. Company Ethic code

Does it exist in your company activity a common mission statement or a company code of ethic?	YES
In this case are these respected by this project?	YES
Is the professional deontology applied in the project development?	YES
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? …………………………………………………. ………………………………………………….	
Did you analyze the ethic's code of the partner companies, checking if it respect the one of your company?	YES
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES
In case an ethic issue have no correspondence on laws or European recommendation, how will you act? ………………………………………………….	

………………………………………………..	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	YES
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	YES
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	NO

UNIVERSITA DEGLI STUDI ROMA TRE

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, 5.

Type of Position	Number of Women	Number of Men
Scientific Coordinator		1
Work package leaders		
Experienced researchers (i.e. PhD holders)	2	2
PhD Students		
Other		

How many additional researchers (in companies and universities) were employed specifically for this project?	1
Of which, indicate the number of women:	1
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES
Did your company carry out specific Gender Equality Actions under the project?	NO
Did your company respect the privacy of employees, correctly treating workers personal data?	YES

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO
In this case, did you report them to the project partners and other stakeholders?	YES / NO / NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behavior between internal and shared working teams?	YES

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? We would discuss the issue with the project coordinator and with the partners in order to find a suitable solution.	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES

F. Company Ethic code

Does it exist in your company activity a common mission statement or a company code of ethic?	NO
In this case are these respected by this project?	YES / NO
Is the professional deontology applied in the project development?	YES
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines? NO	
Did you analyze the ethic's code of the partner companies, checking if it respect the one of your company?	NO
Did your company consider the possible conflicts in international norms and laws involved in the project?	NO
In case an ethic issue have no correspondence on laws or European recommendation, how will you act? We would discuss the issue with the project coordinator and with the partners in order to find a suitable solution.	
Did your company encourage interacting with team, project partner and other	YES

stakeholders in a professional and ethical manner by respecting personal, ethnic, and cultural differences?	
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	NO
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES

G. Environmental issues

Are you taking into account the environment respect and possible environment impact of the project?	NO
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	NO

MYNDIGHETEN FOR SAMHALLSSKYDD OCH BEREDSKAP

A. Workforce Statistics

Please indicate the number of people who worked for your company at the project:	Total, 12.

Type of Position	Number of Women	Number of Men
Scientific Coordinator		
Work package leaders	1	2
Experienced researchers (i.e. PhD holders)		
PhD Students		
Other	4	5

How many additional researchers (in companies and universities) were employed specifically for this project?	NO
Of which, indicate the number of women:	
Do your company respect people working at ISITEP Project, their aspirations, their need to develop their careers, their health and their wellbeing?	YES
Did your company carry out specific Gender Equality Actions under the project?	YES
Did your company respect the privacy of employees, correctly treating workers personal data?	YES

B. Management of the project

Did your company endeavour for ensuring integrity of the project management process?	YES
Did your company encourage team members to conform to the standard of conduct expected for the project?	YES
Did you notice any actions or circumstances that could be construed as a conflict of interest?	NO
In this case, did you report them to the project partners and other stakeholders?	NOT APPLICABLE
Did your company endeavour for ensuring a collaborative behavior between internal and shared working teams?	YES

C. IPR

Did your company respect and protect intellectual property rights of others?	YES
Did your company properly disclose and recognize the professional, intellectual and research contributions employees and of others?	YES

D. Communication between partners

There are usually many ways to realize solutions fulfilling the project requirements. In case a set of candidate solutions have been considered; did your company share them with project partners in order to choose the most convincing solution?	YES
Have your company been clear with partners in highlighting the constraints you encounter during the project, explaining what you will achieve and time needed for obtaining the goals you set?	YES
Did your company follow guidelines for document sharing and dissemination agreed with partners?	YES
In case your company uses particular procedures not compatible with project guidelines, how will you manage the discrepancies? We would discuss the issue with the project coordinator and with the partners in order to find a suitable solution.	

E. Documents treatment

Are all project documents treated as requested by correspondent security classification and security needs?	YES
Have your company correctly applied the international rules to researchers and employees' access to confidential documents?	YES
Have your company correctly applied the international rules to the storage of confidential documents and other research materials?	YES

F. Company Ethic code

Does it exist in your company activity a common mission statement or a company code of ethic?	YES
In this case are these respected by this project?	YES
Is the professional deontology applied in the project development?	YES
Beside eventual legal actions, are disciplinary measures foreseen for people not following project's etic-guidelines?	
Did you analyze the ethic's code of the partner companies, checking if it respect the one of your company?	YES
Did your company consider the possible conflicts in international norms and laws involved in the project?	YES
In case an ethic issue have no correspondence on laws or European recommendation, how will you act?	
Did your company encourage interacting with team, project partner and other stakeholders in a professional and ethical manner by respecting personal, ethnic, and	YES

cultural differences?	
Did your company take into account countries' cultural norms, regulations and legal issues involved in the project framework?	YES
Are "impartiality" and "objectivity" added values guiding your research activity in the project scope?	YES
G. Environmental issues	
Are you taking into account the environment respect and possible environment impact of the project?	YES
During the project developing, have you performed tests or studies taking into account the Electro Magnetic Compatibility Regulation and related environmental and health issues?	NO