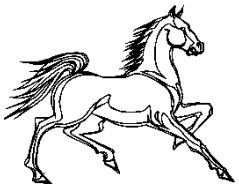

# DESTRIERO

**A DEcision Support Tool for Reconstruction and recovery and for the IntEroperability of international Relief units in case Of complex crises situations, including CBRN contamination risks**

## D2.4 – Preliminary report on ethical issue assessment

Grant Agreement no.: **312721**

Call identifier: **FP7-SEC-2012.4.3-1**

Start date of project: 01/09/2013 Duration: 36 months

| | |
|---|---|
| Deliverable: | D2.4 |
| Title: | Preliminary report on ethical issue assessment |
| Due Delivery Date: | 31st February 2015 |
| Actual Delivery Date: | May 29th, 2015 |
| Lead Contractor for this deliverable: | SELEX-ES |
| Contributor: | CINI, UPVLC, INNO, ITTI |
| Dissemination Level: | PU |
| Version: | 1.0 |
| Document Description: | This document focuses on the assessment of compliance of DESTRIERO with the current EU laws about Ethics, Privacy and Data Protection Issues. |

# Revision History

| Version Number | Description | Date Modified | Author |
|---|---|---|---|
| 0.1 | First Release | 11th March 2014 | V. Esposito<br>F. Matarese |
| 0.2 | Updated release | 12th April 2015 | F. Matarese |
| 0.3 | Paragraph 4.5 and 5.2 | 20th April 2015 | M. Fiorentino |
| 0.4 | Paragraph 4.1, 4.2, 4.3 ,4.4 and 5.1 | 21st April 2015 | M. Rybak |
| 0.5 | Paragraphs 4.6 and 4.7 | 4th May 2015 | J.Gómez Lasquetty |
| 0.6 | Final Draft | 13th May 2015 | F. Matarese |
| 0.7 | Language Review | 29th May 2015 | P. Gmitrowicz |
| 1.0 | Final Version | 29th May 2015 | V. Esposito,<br>D. Dell'Amura |

## TABLE OF CONTENTS

## LIST OF FIGURES



## LIST OF TABLES

## EXECUTIVE SUMMARY

This document summarizes the work carried out in task 2.6 (Ethical Issue Assessment) about DESTRIERO design constraints to be respected in order to avoid privacy issues and to assure compliance with applicable laws. The document is a result of the activities of Work Package 2 (WP2 – PDNA and RRP user requirements).

This document has to clarify which are possible applicable European laws about ethical issues and provide recommendations in order to properly realize the DESTRIERO platform. This analysis has to be considered during design activities provided in D5.1, D5.2, D5.3 and D5.4 and takes care of already available information about user requirements identified in WP2 activities.

In the European Union, privacy and data protection standards include the respect of EU Charter of Fundamental Human Rights and of the EU Data Protection Directive.

The sharing of personal data will be subject to relevant EU standards (e.g. data transfer only to countries able to ensure adequate levels of data protection).

Technologies that are planned to be used within the project will satisfy all the relevant laws and ethical regulations. Especially privacy and data security are in the centre of attention. The project consortium commits itself to carry out all research activities in strict conformity with EU and national legislation and regulations, and to comply with the Charter of Fundamental Rights (2000) of the EU in respect to the citizen's dignity, freedom, equality, rights, and justice.

In order to properly study current European Union laws and to provide possible recommendations for next design phases, three main activities have been identified and will be provided in next chapters:

- Analysis of National and European privacy and data protection regulations
- Analysis of data protection issues in a collaborative environment
- Initial Recommendations definition

# 1 INTRODUCTION

The purpose of this document is to provide an assessment of compliance of DESTRIERO with the current laws and directives (national and EU) about Ethics, Privacy and Data Protection Issues.

This deliverable will be used as an intermediate report on Privacy and Ethical aspects assessment and identifications of recommendations for DESTRIERO system implementation.

The deliverable is a report of Task 2.6, in the frame of WP2 (*PDNA and RRP user requirements*).

T2.6 objectives are to:

- provide guidelines for ethical issues management in the frame of DESTRIERO project, and
- ensure the privacy of the people, whose data or images could be treated during the project.

In particular, activities of T2.6 are related to:

- the identification of ethical issues and constraints, which could potentially impact the functionality of DESTRIERO system, and
- the assurance of compliance with applicable national laws and EU regulations for privacy and data protection, in order to guarantee that the privacy and ethical aspects of the EU citizens would not be threatened anyhow by the DESTRIERO approach and technologies.

## *1.1 Document Organisation*

This document is divided in the following sections:

**Chapter 2 –** Analysis of national and European privacy and data protection regulations.
**Chapter 3** – Evaluation of privacy and data protection issues in DESTRIERO collaborative environment
**Chapter 4 -** Definition of Recommendations to manage potential identified Ethical Issues

## *1.2 Description of Work*

In order to meet the above objectives, the following sub-tasks are performed:

- Overview of National and European privacy and data protection regulations
  - Identification of National and European privacy and data protection regulations,
  - Analysis of National and European privacy and data protection regulations,
- Identification of privacy and data protection issues in a collaborative environment
  - Identification of privacy and data protection issues in DESTRIERO demonstration scenario,

  - Analysis of legal requirements related to identified issues,
- Definition of Initial Recommendations
  - Assessment of user requirements and functional specifications,
  - Assessment of DESTRIERO compliance toward regulations,
  - Definition of recommendations to guarantee ethical issues are not violated.

This deliverable has the objective of preliminary assessment of potential impact of ethical issues on DESTRIERO and definition of recommendations for the design and development of the demonstrator, in compliance with national and EU regulations on data protection.

This deliverable is the input for Deliverable D2.5 and Architecture Design (WP5) and Development of platform for PDNA and RRP (WP6).

## *1.3 Partners*

The DESTRIERO partners on the task 2.6 contributed in the following areas:

| Partner | Major Task |
|---|---|
| SESM | • Task Management |
| CINI | • Overview of National and European privacy and data protection regulations<br>• Identification of privacy and data protection issues in a collaborative environment |
| UPVLC | • Overview of National and European privacy and data protection regulations<br>• Analysis of Recommendations to manage Ethical Issues |
| INNO | • Identification of privacy and data protection issues in a collaborative environment<br>• Definition of Initial Recommendations to manage Ethical Issues |
| ITTI | • Overview of National and European privacy and data protection regulations<br>• Identification of privacy and data protection issues in a collaborative environment |

**Table 1 - DESTRIERO Partners' role**

## *1.4 Reference Documents*

| Document name |
|---|
| [1] UNDP, Bollin, C. and Khanna, S (2007), "Review of Post Disaster Recovery Needs Assessment and Methodologies", available at: http://www.saludydesastres.info/ |

| Document name |
|---|
| [2] DESTRIERO – ANNEX 1: Description of Work – Grant Agreement n° 312721 |
| [3] DESTRIERO User Requirements Questionnaire |
| [4] European Union, Regulations, Directives and other acts, available online at http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm |
| [5] European Union (2009), Directive 2009/136/EC of the European Parliament and of the Council, available online http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1429525026499&uri=CELEX:32009L0136 |
| [6] European Union (2008), Council Framework Decision 2008/977/JHA, available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1414070625251&uri=CELEX:32008F0977 |
| [7] European Union (2002), Directive 2002/58/EC of the European Parliament and of the Council, available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1414072277428&uri=CELEX:32002L0058 |
| [8] European Union (1995), Directive 95/46/EC of the European Parliament and of the Council, available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT |
| [9] Jerry Kang (1998), Information Privacy in Cyberspace Transactions, Stanford Law Review, Vol. 50, No. 4, pp. 1193-1294 |
| [10] Jed Rubenfeld (1989), The Right of Privacy, Harv. L. Rev. 737, 784 |
| [11] UPVLC (2013): D2.2 – Detailed Scenario definition. DESTRIERO deliverable to T2.3. |
| [12] SELEX-ES (2015): D5.2 – Adapter Design |
| [13] Privacy Working Group (1998), Information Infrastructure Task Force Principles, Clinton Administration |
| [14] CINI (2015): D5.3 – Design of tools extensions and new capabilities |
| [15] M. F. Dennedy, J. Fox, T. Finneran (2014), The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value, Apress, pag. 218-220 |

| Document name |
|---|
| [16] European Union Agency for Fundamental Rights: *Handbook on European data protection law*, 2013. |
| [17] Gunnar Beck: The EU Charter of Fundamental Rights – An overview [in:] The application of the EU Charter of Fundamental Rights to asylum procedural law, October 2014. |

## *1.5 Table of Acronyms*

| Acronym | Description |
|---|---|
| **DPO** | Data Protection Officer |
| **EDPS** | European Data Protection Supervisor |
| **EU** | European Union |
| **NGO** | Non-Governmental Organisation |
| **OCHA** | Office for the Coordination of Humanitarian Affairs (UN) |
| **PDNA** | Post Disaster and Needs Assessment |
| **RRNA** | Rapid Recovery Needs Assessment |
| **RRP** | Reconstruction and Recovery Planning |
| **SOTA** | State of the Art |
| **UNDP** | United Nations Development Programme |
| **WP** | Work Package |

# 2 NATIONAL AND EUROPEAN PRIVACY AND DATA PROTECTION REGULATIONS

The process of IT system development often requires a contact with End-Users to collect their needs and expectations (requirements) regarding the future system. To properly manage those requirements and analyse them, some personal data (e.g. demographic) about End-Users should have also been collected and processed.

Personal data allow to recognise, locate and contact a single person on basis of them, therefore should be protected against unauthorised access to protect privacy and safety of a single person. In this case, identification of threats and implementation of adequate procedures to prevent them is a must.

Data gathered from End-Users in the project indeed is personal data, since the following have been collected:

- End-Users name and surname,
- Organisation they work for,
- E-mail,
- Telephone number.

However, it is not sensitive data (pertaining to health, race, sexual orientation, political, philosophical or religious views), which might be potentially a cause of persecution. These types of data are not and will not be collected in the project (since they are not needed).

To prevent any potentially dangerous situations, the adequate security and protection of data procedures, which are well described within the European law, have been implemented. In DESTRIERO project, safety of gathered data as well as safety of responders is important, therefore compliance with the law regulations and ethical aspects (good practices) have been checked to guarantee that none will get violated.

## *2.1 Charter of Fundamental Right of the European Union*

The Charter of Fundamental Right of the European Union was proclaimed in 2000 by the European Parliament, the Council and the Commission to systematise fundamental rights of citizens of European Union. Chart was made to protect social, political and economic rights for European Union citizens and residents into European Union law. "Within the framework of EU law, it has a higher normative status than all EU legislation adopted under the Treaties and all national laws implementing Union law" [Beck, 2014].

This Charter is subdivided to the few titles (chapters):

1 **Title I: Dignity** – describes human dignity, right to life, integrity of the person, prohibition of torture and inhuman treatment, prohibition of slavery and forced labour.

2 **Title II: Freedoms** – covers the right to liberty and security, respect for private and family life, including personal data, freedom of thought, conscience and religion, freedom of expression and information and personal integrity, privacy and the right to asylum.

1 **Title III: Equality** – includes right to equality before the law and non-discrimination, cultural, religious and linguistic diversity, respect for the child and the elderly, as well as integration of persons with disabilities.

2 **Title IV: Solidarity** – guarantees workers' rights, prohibition of child labour and protection of young people at work, social security and assistance, access to services of general economic interest and health care, environmental and consumer protection.

3 **Title V: Citizens' Rights** – states that all EU citizens have rights to vote, stand as a candidate at election, good administration, access to documents, Ombudsman, freedom of movement and of residence and diplomatic and consular protection.

4 **Title VI: Justice** – covers right to effective remedy and to a fair trial, principles of legality and proportionality of criminal offences and penalties.

5 **Title VII: General provisions governing the interpretation and application of the charter** – contains of instructions how to read and use the Charter, to properly interpret and use it.

Each of those chapters (titles) describes a various areas of human rights and life. In DESTRIERO project, a special attention should be given to Title II, where freedoms of man have been specified. All articles in this Title in Charter of Fundamental Right of the European Union are centred upon the rights of freedom and personal secure. In the context of DESTRIERO project, the Article 8 seems to be the most relevant (quoted below).

"*Article 8 - Protection of personal data:*

1 *Everyone has the right to the protection of personal data concerning him or her.*
2 *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the rights of access to data which has been collected concerning him or her, and the right to have it rectified.*
3 *Compliance with these rules shall be subject to control by an independent authority."*

The article highlights that everyone's data should be protected and data processing should be preceded by a consent (or other legitimate basis) of the person concerned. It is the most relevant for the requirements gathering and analysing process (within WP2 and WP5 – HMI development).

In DESTRIERO project, responders' data are stored on separate, project hard drives and are kept secure from any potential abuses. Paper versions of the questionnaires are stored safely and only a small group of persons within Consortium has the access to them. The electronic version of them (.xls) is secured with a password and available only for members who have been engaged in analyses process or requirements tracking.

Personal data are and will be used for project purposes only. They are treated with the strictest level of confidentiality and will never be disclosed to any third party. All data were gathered and processed on basis of voluntary consent of End-Users.

Another important point in the quoted Article 8 is an access to data concerning a particular person, which should be allowed to them, as well as a right to rectify those data.

End-Users have the right to access and therefore rectify data which concern them. They might do it through the Governance and End-Users Board which is led by ITTI. The communication procedures through the Governance and End-Users Board are described in D1.3. The Governance and End-Users Board should be considered as a contact point for End-Users, where all of the actual issues on the line Consortium-End-Users might be reported and resolved.

According the DoW, which states that: "The Governance and End-Users Board [...] is in the charge of supervising: [...] Analysis of governance, legal, ethical and gender issue related to information exchange among different entities with different protocols", the Board has also a role of independent authority which takes care of compliance with rules mentioned in the Article 8, paragraph 3.

## *2.2 European Convention on Human Rights*

European Convention on Human Rights is an international treat which aims to protect human rights, fundamental, democratic freedoms and social development among Europe. States are internationally obligated to comply with the Convention.

The Convention consists of three sections:

1 **Section I – Rights and Freedoms** – defines basic rights like: right to life, prohibition of torture, slavery and forced labour, right to liberty and security, fair trial, no punishment without law, respect for private and family life, freedom of thought, conscience, religion, expression, assembly and association, effective remedy, prohibition of discrimination and abuse of rights.
2 **Section II – European Court of Human Rights** – sets up the Court and defines its rules of operation.
3 **Section III – Miscellaneous provisions** – contains concluding provisions.

For the DESTRIERO project, the Article 8 is applicable, where the right for a private and family life is stated, since it might have also an impact for a gathering a personal data by questionnaires.

*"Article 8 – Right to respect for private and family life.*

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

This paragraph obligates project members to storage gathered, personal data safety to prevent any possibility of data leakage which might threaten a private life of a single person

and to never disclosed them to any third party. Responders (End-Users) have the right to their private life which includes the respect for their private, personal data.

## *2.3 Council of Europe Convention 108*

Council of Europe Convention 108: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* is intended to extend the safeguards for everyone's rights and fundamental freedoms. It is deemed that the Convention 1-8 is referring to Article 8 of the European Convention on Human Rights (described in chapter 2.2) and "remains the only legally binding international instrument in the data protection field" [European Union Agency for Fundamental Rights, 2013].

The Convention is divided into 7 chapters:

1 **Chapter I: General provisions** - describes basic information about rights of freedoms and privacy.
2 **Chapter II: Basic principles for data protection** - defines categories of personal data and how to protect them.
3 **Chapter III: Trans-border data flows** - describes how Member States should cooperate.
4 **Chapter IV – Mutual assistance** - establishes Consultative Committee and its functions.
5 **Chapter V – Consultative Committee** - covers all amendments for this convention.
6 **Chapter VI – Amendments** - describes all changes provided for this convention.
7 **Chapter VII – Final clauses** - – includes information when convention entry into force, territorial clause etc.

The most relevant from the project's point of view is chapter II: "*Basic principles for data protection"*. There are 8 articles, and Articles: 5, 6 and 7 deserve more attention to be paid.

Article 5 refers to quality of data, in particular that they must be processed fairly, be adequate, relevant and preserved in form of personal data for no longer than required.

> *"Article 5 – Quality of data*
>
> *Personal data undergoing automatic processing shall be:*
>
> *a. Obtained and processed fairly and lawfully;*
>
> *b. Stored for specified and legitimate purposes and not used in a way incompatible with those purposes;*
>
> *c. Adequate, relevant and not excessive in relation to the purposes for which they are stored;*
>
> *d. Accurate and, where necessary, kept up to date;*
>
> *e. Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."*

A special attention should be given to the Article 5, Paragraph c, which describes that gathered data should be in relation to the purposes of the project. In DESTRIERO project, the

rule of "minimum information" has been respected. It means that only needed data (and no more) have been gathered. During the workshops and surveys with End-Users only the basic personal data have been collected (which are described in the beginning of chapter **Errore. L'origine riferimento non è stata trovata.**). Collection of personal data was voluntary and with the consent of End-Users.

Another article describing the rules of processing data is the Article 6. However, it contains restrictions for a special type of data: concerning racial origin, political opinions, religious beliefs, sexual preference (sensitive data).

> *"Article 6 – Special categories of data*
>
> *Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."*

This article is not relevant for DESTRIERO, since no sensitive data have been (nor will be) needed in the project, therefore – they are not gathered.

Next article which pertains to data security is the Article 7 – named – "*Data security*", this article describes that gathered data must be protected against accidental or unauthorised destruction or loss.

> *"Article 7 – Data security*
>
> *Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."*

In the project the data are protected from unauthorised dissemination, alteration and access. Files which include personal data are available only for a small group of the Consortium members. They are presented to the widely audience only in anonymous form, which does not allow to recognise a single person on their basis (therefore they are no longer personal data, according to the definition). All these files have been exchanged only as part of the DESTRIERO project. No security incident/abuse has been registered during a data processing.

## *2.4 Treaty*

*Treaty on the Functioning of the European Union* was written by the rule authorities of Member States and describes how the European Union should have been organised. The Treaty is split into seven parts.

1. **Part one: Principles** - This part describes basis legal of the European Union and its assumptions.
2. **Part two: Non-discrimination and citizenship of the Union** - All articles contained in this part describes rights of citizens of European Union.
3. **Part three: Union policies and internal actions** – This part is about following titles: the internal market, the free movement of good, including the customs union, and more.

4 **Part four: Association of the overseas countries and territories** – This part deals with association of overseas territories.
5 **Part five: The union's external actions** – This part deals with all activities outside Unions border.
6 **Part six: Institutional and financial provisions** – In this part are described institutions of European Union for example articles 300 to 309 establish the European Investments Bank.
7 **Part seven: General and final provisions** – Last part of Treaty is about final legal points.

From all these parts, the part one has a value in the context of the project. Article 16 contains a general EU competence to legislate on data protection matters:

"*Article 16 (ex Article 286 TEC (Treaty Establishing the European Community))*

1 *Everyone has the right to the protection of the personal data concerning them.*
2 *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*

*The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."*

The first paragraph of the Article establishes the basis of Common law of protection of personal data, which means that all activities of processing personal data in project underlie this law.

The second paragraph guarantees the independence of data protection authorities, which is fundamental element of the right to data protection.

Article 16 invokes article 39 of Treaty on European Union:

*"Article 39*

*In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."*

## *2.5 Directives & Framework Decisions*

This section provides an overview of the European Union framework directives and decisions that regulate the processing of personal data and the protection of privacy. To completely

understand the analysis here proposed, a definition is provided and used hereinafter concerning the concept of framework "decision" and "directive".

*"A directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how"* [4]. This was the case with the working time directive, which stipulates that too much overtime work is illegal. The directive sets out minimum rest periods and a maximum number of working hours, but it is up to each country to devise its own laws on how to implement this.

"*A decision is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable"* [4]. For example, when the Commission issued a decision fining software giant Microsoft for abusing its dominant market position, it applied to Microsoft only. Despite the abolition of their legal basis, Framework Decisions are still valid and should be taken into account according to the Art. 9 para. 1 of Protocol N° 36 attached to the Treaty of Lisbon, which says: "The legal effects of the acts of the institutions, bodies, offices and agencies of the Union adopted on the basis of the Treaty on European Union prior to the entry into force of the Treaty of Lisbon shall be preserved until those acts are repealed, annulled or amended in implementation of the Treaties. […]".

In the field of data protection and human privacy the European Parliament has produced in the 1995 an official directive (95/46/EC) in which the main topic addressed was the protection of individuals regarding personal data. This directive has changed during these years by adopting a series of extensions (2002/22/EC and 2002/58/EC) and amendment (2009/136/EC). On 2008 also the framework decision (2008/977/JHA) has been issued on the topic. Schematically this can be summarized as follows:

- **Directive**:
    1. *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [8].
    2. *Directive 2002/22/EC* on universal service and users' rights relating to electronic communications networks and services [5],
    3. *Directive 2002/58/EC* concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [7],
- **Decision**:
    1. *Council Framework Decision 2008/977/JHA* of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [6].

The analysis of the directives 2002/22/EC and 2002/58/EC has been conducted by taking into account the amendments defined into the *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009*. This is a consequence of the fact that the functioning of all the directives and the decision above-reported are subject to periodic review by the Commission so that they can be updated with the technological and market developments. In the next paragraph it is provided a summary of above directives and the

decision, for further details please refer to the references provided at the beginning of the document.

### 2.5.1 Directive 95/46/EC

The objective of the directive 95/46/EC of the European parliament and of the council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, is twofold [8]:

1. Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the *processing of personal data*.
2. Member States shall neither restrict nor prohibit the free flow of *personal data* between Member States for reasons connected with the protection afforded under paragraph.

Where:

- "personal data" means any information relating to an identified or identifiable natural person ('data subject');
- "processing of personal data" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

The main responsibilities of this directive are related to the protection of the end-user personal data when this is processed by automatic machines or by other means not completely automatic such as filing systems.

In the following we summarize the articles of the directive that are particularly relevant in the context of the DESTRIERO project:

- *Article 6 Member States shall provide that personal data must be:*
  - processed fairly and lawfully;
  - collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes […],
  - adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
  - accurate and, where necessary, kept up to date; […];
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
- *Article 12 Right of Access*, "Member States shall guarantee every data subject the right to obtain from the controller:
  - without constraint at reasonable intervals and without excessive delay or expense:

        - confirmation as to whether or not data relating to them are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed ,
        - communication to them in an intelligible form of the data undergoing processing and of any available information as to their source,
        - knowledge of the logic involved in any automatic processing of data concerning them at least in the case of the automated decisions referred to in Article 15;
    - as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
    - notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort."
- *Article 17 Security of processing*,
    - Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. […].
    - The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
    - The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller […].
    - For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures shall be in writing or in another equivalent form.
- *Article 25 Principles*,
    - The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
    - The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectorial, in force in the third

country in question and the professional rules and security measures which are complied with in that country.

### 2.5.2 Directive 2002/22/EC

The directive 2002/22/EC of the European Parliament and of the council of 7 March 2002 concerns the provision of electronic communications networks and services to End-Users. Furthermore, the directive is intended to deal with circumstances in which the needs of the End-Users are not satisfied at all by the market. Finally, it also includes provisions concerning aspects of terminal equipment, for example the provisions to facilitate access for disabled End-Users. The directive does not directly address the protection of sensible data and privacy, but some articles could be of interest for the objectives of the DESTRIERO project:

- *Article 21 (Transparency and publication of information)* "Member States shall ensure that national regulatory authorities are able to oblige undertakings providing public electronic communications networks and/or publicly available electronic communications services to publish transparent, comparable, adequate and up-to-date information on applicable prices and tariffs, on any charges due on termination of a contract and on standard terms and conditions in respect of access to, and use of, services provided by them to End-Users and consumers."
- *Article 22 (Quality of Service) – point 1: "*Member States shall ensure that national regulatory authorities are, after taking account of the views of interested parties, able to require undertakings that provide publicly available electronic communications networks and/or services to publish comparable, adequate and up-to-date information for End-Users on the quality of their services and on measures taken to ensure equivalence in access for disabled End-Users. That information shall, on request, be supplied to the national regulatory authority in advance of its publication". Point 2, differently, says that for preventing the degradation of service and the hindering or slowing down of traffic over networks, "Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks".

Furthermore, several references are made to the directive 2002/58/EC that is introduced in the next paragraph and that specifically addresses the topic of data protection and privacy.

### 2.5.3 Directive 2002/58/EC

The main role of this directive is to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, by taking into account processing of personal data in the electronic communication sector. Furthermore, the directive addresses also the ways to let this data be moved within the Community. The directive refers to different topics but the ones that should be taken into account in DESTRIERO are: security (Article 4), confidentiality of the communications (Article 5), traffic data (Article 6), and location data different from traffic data (Article 9). The other articles do not impact directly on the DESTRIERO infrastructure and so have not been taken into account.

- *Article 4 (Security) – point 1*, "the provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented". Whereas point 2 says that "in case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved."
- *Article 5 (Confidentiality of the Communication)*, Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit **listening**, **tapping**, **storage** or other kinds of **interception** or **surveillance** of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised."
- *Article 6 (Traffic Data),* traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.
- *Article 9 (Location data other than traffic data), "*where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time."

### 2.5.4 Council Framework Decision 2008/977/JHA

The council framework decision 2008/977/JHA of 27 November 2008, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, can be considered as an extension to the previous introduced concepts about the directives to achieve personal data privacy in communications networks and services. In fact, this decision, differently from the directives above defined, is specifically designed to be applied in the framework of police and judicial cooperation. As stated in Article 1, in accordance with this Framework Decision, "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy when, for the

purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, personal data:

- are or have been transmitted or made available among Member States;
- are or have been transmitted or made available by Member States to authorities or to information systems established on the basis of Title VI of the Treaty on European Union; or
- are or have been transmitted or made available to the competent authorities of the Member States by authorities or information systems established on the basis of the Treaty on European Union or the Treaty establishing the European Community. "

Also for this decision we have summarized all the relevant articles that could be of interest in the DESTRIERO project:

- *Article 3 Principles of lawfulness, "*personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected."
- *Article 4 Rectification, erasure and blocking,*
    - Personal data shall be rectified if inaccurate and, where this is possible and necessary, completed or updated.
    - Personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed. Archiving of those data in a separate data set for an appropriate period in accordance with national law shall not be affected by this provision.
    - Personal data shall be blocked instead of erased if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose that prevented their erasure.
    - When the personal data are contained in a judicial decision or record related to the issuance of a judicial decision, the rectification, and erasure or blocking shall be carried out in accordance with national rules on judicial proceedings.
- *Article 21 Confidentiality of processing*, "Any person who has access to personal data which fall within the scope of this Framework Decision may process such data only if that person is a member of, or acts on instructions of, the competent authority, unless he is required to do so by law."
- *Article 22 Security of processing*, "Member States shall provide that the competent authorities must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission over a network or the making available by granting direct automated access, and against all other unlawful forms of processing, taking into account in particular the risks represented by the processing and the nature of the data to be protected. Having regard to the state of the art and the cost of their

implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

If the articles here presented and the ones that fully characterize the summarized decision are not adopted, Member States shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Framework Decision, according to the article 24.

## *2.6 Regulation*

This section provides an overview on the regulation No 45/2001 of the European Parliament and the Council of the European Union of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

A Regulation is necessary to provide the individual with legally enforceable rights, to specify the data processing obligations of the controllers within the Community institutions and bodies, and to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies

The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever, for example because they are employed by those institutions or bodies.

The principles of data protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the said person. The principles of protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

Directive 95/46/EC requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, in order to ensure the free flow of personal data in the Community.

In accordance with this Regulation, the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities, hereinafter referred to as 'Community institutions or bodies', shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC.

This Regulation shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

General rules on the lawfulness of the processing of personal data and the criteria for data quality and making the data processing legitimate are described in the following sections.

### 2.6.1 Data quality

Personal data must be:

- Processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

### 2.6.2 Data processing

Personal data may be processed only if:

- Processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- The data subject has unambiguously given his or her consent
- Processing is necessary in order to protect the vital interests of the data subject.

### 2.6.3 Change of purpose

Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body.

Personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences.

### 2.6.4 Transfer of personal data within or between Community institutions or bodies

Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient. Where the data are transferred following a request from the recipient, both the controller and the recipient shall bear the responsibility for the legitimacy of this transfer.

The recipient shall process the personal data only for the purposes for which they were transmitted.

### 2.6.5 Transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC

Personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC if:

- The recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority.
- The recipient establishes the necessity of having the data transferred and if there is no reason to subject's legitimate interests might be prejudiced.

### 2.6.6 Transfer of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC

Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.

### 2.6.7 The processing of special categories of data

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, is prohibited.

The above paragraph shall not apply when:

- The data subject has given his or her express consent to the processing of those data
- Processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent
- Processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Community institution or body, not subject to national data protection law by virtue of Article 4 of Directive 95/46/EC, and with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.
- Processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy.

## 2.7 Data protection bodies

Article 286 of the Treaty establishing the European Community requires the application to the Community institutions and bodies of the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data. This article also requires the establishment of an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies. In the other hand, the member states have their own national data protection authorities.

### 2.7.1 National Data Protection Authorities

National data protection authorities for the European Union members are gathered together in the following list:

- Austria: Österreichische Datenschutzbehörde
- Belgium: Commission de la protection de la vie privée
- Bulgaria: Commission for Personal Data Protection
- Croatia: Croatian Personal Data Protection Agency
- Cyprus: Commissioner for Personal Data Protection
- Czech Republic: The Office for Personal Data Protection
- Denmark: Datatilsynet
- Estonia: Estonian Data Protection Inspectorate
- Finland: Office of the Data Protection
- France: Commission Nationale de l'Informatique et des Libertés
- Germany: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Greece: Hellenic Data Protection Authority
- Hungary: Data Protection Commissioner of Hungary
- Ireland: Data Protection Commissioner
- Italy: Garante per la protezione dei dati personali
- Latvia: Data State Inspectorate
- Lithuania: State Data Protection
- Luxembourg: Commission nationale pour la protection des données
- Malta: the Data Protection Commissioner
- The Netherlands: College bescherming persoonsgegevens
- Poland: The Bureau of the Inspector General for the Protection of Personal Data
- Portugal: Comissão Nacional de Protecção de Dados
- Romania: The National Supervisory Authority for Personal Data Processing
- Slovakia: Office for Personal Data Protection of the Slovak Republic
- Slovenia: Information Commissioner
- Spain: Agencia de Protección de Datos
- Sweden: Datainspektionen
- United Kingdom: The Information Commissioner's Office

### 2.7.2 European Data Protection Supervisor

The Regulation on the protection of individuals with regard to the processing of personal data by EU institutions establishes a European Data Protection Supervisor (EDPS). This is an independent EU body responsible for monitoring the application of data protection rules within European Institutions and for investigating complaints.

The EDPS works at the European level, and is similar to national data protection authorities across the EU. Individuals can lodge complaints directly with the EDPS, if they consider that their data protection rights have been ignored.

The EDPS can hear and investigate complaints, monitor and ensure that the Regulation is applied and advise EU institutions and bodies on everything about processing personal data.

The European Commission must consult the EDPS when adopting legislative proposals relating to the processing of personal data in any sector.

### 2.7.3 EU Data Protection Officer

The Regulation on the protection of individuals with regard to the processing of personal data by EU institutions provides for the appointment of a Data Protection Officer (DPO) in every EU institution.

A Data Protection Officer (DPO) in every EU institution and body works closely with the EDPS to ensure the internal application of the Regulation on the protection of individuals with regard to the processing of personal data by EU institutions.

The task of DPOs is to independently ensure the internal application of the Regulation in close cooperation with the European Data Protection Supervisor.

# 3 PRIVACY AND DATA PROTECTION ISSUES IN DESTRIERO COLLABORATIVE ENVIRONMENT

## *3.1 Identification of user requirements and functional specifications related to data protection*

Possible problems related to databases, data storage and protection were identified during comparatively early stage of the project. Thanks to that, it was possible to include the adequate sections in the requirements gathering tool (questionnaire) which were exploring those issues wider. Moreover, privacy and data protection issues were also discussed during the workshop in Paris.

Full set of the collected requirements has been already submitted in D2.1, in the chapter 4: Formalization and prioritization of collected user requirements. Requirements in this deliverable were split into the seven main categories:

- General requirements.
- Database and storage requirements.
- Communication requirements.
- HMI requirements.
- Hardware requirements.
- Ethical requirements.
- Collaborative work requirements.

Comparatively small group of the requirements was connected to the data protection, but it does not mean that a lower attention should be devoted to this subject. Almost all of the identified requirements in this area were classified as a "critical", only one as a "serious". What is interesting, the identified by responders potential risks with data and privacy cannot be assigned only to the "database and storage requirements" group, but also to the Communication, Ethical, and Collaboration groups. It proves that responders (as well as Consortium) were highly aware of the multidimensional nature of the problem.

According to the collected feedback, the level of access to particular data and features should be differenced by users' role. It means that there is a need to establish different levels of access (and establishing it should allow by). It also requires user authentication mechanisms, which would protect data from unauthorised access. The following requirements address those issues:

| ID | DATABASE_req#003 | Importance | Critical |
|---|---|---|---|
| Name | User authorization | | |
| Type | Non-functional | Sub-type | Security |
| Source | DESTRIERO questionnaire | Version | 0.1 |
| Description | Only authorized DESTRIERO users shall access to the DESTRIERO data. | | |
| Comment | For example, no third parties shall be able access DESTRIERO without authorization. | | |

**Figure 1 - DATABASE_req#003**

| ID | DATABASE_req#004 | Importance | Critical |
|---|---|---|---|
| Name | User authentication process | | |
| Type | Functional | Sub-type | Functional |
| Source | DESTRIERO questionnaire | Version | 0.1 |
| Description | Access to stored data shall be done by means of an authentication process. | | |
| Comment | Authorization and authentication processes shall be performed to all user attempting access to the DESTRIERO. | | |

**Figure 2 - DATABASE_req#004**

| ID | COMMUNICATION_req#014 | Importance | Critical |
|---|---|---|---|
| Name | Access rights | | |
| Type | Non-functional | Sub-type | Security |
| Source | Paris Workshop 12 Dec 2013 | Version | 0.1 |
| Description | The system shall allow organizations involved in reconstruction to define access rights for information they uploaded. Especially an organization must be able to define who may access its data. | | |
| Comment | Some data needed for reconstruction may be sensitive or classified. Therefore without appropriate privilege management the system may be forbidden to be uses by law. | | |

**Figure 3 - COMMUNICATION_req#014**

| ID | ETHICAL_req#001 | Importance | Critical |
|---|---|---|---|
| Name | Secure data storage | | |
| Type | Non-functional | Sub-type | Legal |
| Source | DESTRIERO questionnaire | Version | 0.1 |
| Description | The system shall store sensitive data securely. | | |
| Comment | DESTRIERO shall ensure that all critical and sensitive data are secure and no unauthorized user could have access to it. | | |

**Figure 4 - ETHICAL_req#001**

There were also the requirements (from the Communication and Ethical areas) which highlight the importance of meeting with EU and national laws regulations, especially those regarding sensitive data.

| ID | COMMUNICATION_req#017 | Importance | Critical |
|---|---|---|---|
| Name | IT Security | | |
| Type | Non-functional | Sub-type | Security |
| Source | Paris Workshop 12 Dec 2013 | Version | 0.1 |
| Description | The system shall provide adequate IT protection against data stealing and data forging. | | |
| Comment | Some data needed for reconstruction may be sensitive or classified. Therefore without appropriate IT security level the system may be forbidden to be uses by law. | | |

**Figure 5 - COMMUNICATION_req#017**

| ID | ETHICAL_req#002 | Importance | Critical |
|---|---|---|---|
| Name | EU regulations compliance | | |
| Type | Non-functional | Sub-type | Legal |
| Source | DESTRIERO questionnaire | Version | 0.1 |
| Description | The system shall meet EU regulations and national laws regarding sensitive data. | | |
| Comment | The system shall not violate any EU regulations. | | |

**Figure 6 - ETHICAL_req#002**

Also a security of the information during the data flow between agencies was not skipped. Requirements presented below express this:

| ID | COLLABORATIVE_req#004 | Importance | Serious |
|---|---|---|---|
| Name | Intra agencies work flow | | |
| Type | Non-functional | Sub-type | Operational |
| Source | DESTRIERO questionnaire | Version | 0.1 |
| Description | The system shall shows bound and automate work flows inside and between recovery and reconstruction agencies. | | |
| Comment | The data flow between agencies shall be automated and secure. | | |

**Figure 7 - COLLABORATIVE_req#004**

## *3.2 Identification of privacy and data protection issues in DESTRIERO demonstration scenario*

According to [9], the term "privacy" conveys numerous ideas that can be clustered in three groupings:

- **Space**: related to the physical space, in particular, "the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals",
- **Decision**: privacy is concerned with choice, "an individual's ability to make certain significant decisions without interference",
- **Information**: concerns the flow of personal information. It is related to the capability of an individual to have control over the processing of personal information (i.e. acquisition, disclosure and use).

By analysing [9] and [10], the entire three grouping can convey into a single, abstract cluster grounded in some moral value such as:

- Human Dignity,
- Inviolate Personality,
- Socio psychological Process (i.e. interpersonal boundary maintenance),
- Political Theory (i.e. anti-totalitarianism).

Considering the European Parliament decisions and directives, defined in §4.5 and related to the data protection and privacy of individuals when consuming services, we will focus on the third defined group. To be more precise, we provide here a detailed definition of information privacy that will be used to approach the security and data protection issues in the demonstration scenario: "an individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed, and used" ([13]).

The approach that has been used for the analysis of the data protection and privacy issues can be characterized in two steps:

1. A first identification of all the services exposed by the platform and external systems (e.g. information sources or third party systems) by limiting them to those needed for the demonstration scenario workflow. The services' assessment has been conducted analysing the deliverable [12] and [14], output of the T5.2 and T5.3 activities respectively,
2. A detailed assessment, for the identified entities in point (1), about the possible data protection and privacy issues according to the privacy topics identified previously and in [15].

For each identified service/system we have tried to understand if what has been done till now meet or exceed the privacy and data protection requirements defined in section §5.1 by answering to the following questions ([15]):

- **Data**:
  - What data is involved?
  - Are they sensitive?

  - Do they constitute the minimum necessary?
- **Purpose**:
  - How and why is the data processed?
- **Means of Collection**:
  - How is the data acquired?
- **Notice**:
  - Is a notice been provided?
  - Did it adequately explain how the personal information would be processed?
- **Access**, **Correction**, **Deletion**:
  - Does the user have a means of accessing his or her personal information and the ability to correct or delete?

The results of the proposed methodology are exposed in Table 2. All the aspects related to the accountability concepts have not been taken into account due to the fact that these concepts are currently further elaborated in the T5.5 activity.

For each of the service/system presented, a level as been assigned that indicates, among four possible values (None, Low, Medium, High), the level of data protection and privacy that has been currently achieved at the current stage of the DESTRIERO project in respect to the European Parliament directive and decisions.

- **None**: indicates that no privacy or data protection means have been provided for a specific service,
- **Low**: this level represent the fact that not all the points of the directives and decisions are covered for the analysed service,
- **Medium**: indicates that directives and decisions have been almost covered,
- **High**: directives and decisions have been totally covered according to the interested articles (refer to paragraph §4.2).

To validate assigned values it is possible to find, added to Table 2, other two columns that represent the coverage to the European Parliament directives and decisions, in terms of article, that have been satisfied or not.

By looking at Table 2 some privacy issues, for some of the exposed services, are putted in evidence. This should not alarm because most of the uncovered aspects will be detailed and further explored during the activities T5.5 concerning the identification and characterization of reliable and secure mechanisms to be implemented into the DESTRIERO platform in order to meet reliable and secure requirements defined in the context of the T2.1 activity.

| Service | Sensitive Data | Data acquisition process | Source | Access, Correction, Deletion | Personal Information Notice | 95/46/EC Coverage | 2002/58/EC Coverage | Level |
|---|---|---|---|---|---|---|---|---|
| **Damage Assessment - Social** | Account and published data (i.e. images, post or videos) | All the data is acquired through the Geo Crowdsourcing tool, provided by EGEOS. No data is stored within the platform. | Social Networks such as Facebook and Twitter | No | N.A. | N.A | N.A | **NONE** |
| **Damage Assessment - Upload Information** | Private Reports | The user himself uploads through the HMI the document/report/file that he wants to put into the platform | Data is gathered from the field and then a report is created and uploaded | Yes, to all | N.A. | Article 6, 12, 17 are covered<br>Article 25 is not covered | Article 4, 5, 6 are covered in [D5.5]<br>Article 9 is not covered | **MEDIUM** |
| **Activity Management** | Organization's data | An organization decides to start a new plan, and then creates all the activities. The plan information are shared through the DESTRIERO infrastructure | Data is created within the DESTRIERO HMI | Yes, to all | N.A | Article 6, 12, 17 are covered<br>Article 25 is not covered | Article 4, 5, 6 are covered in [D5.5]<br>Article 9 is not covered | **MEDIUM** |

| Service | Sensitive Data | Data acquisition process | Source | Access, Correction, Deletion | Personal Information Notice | 95/46/EC Coverage | 2002/58/EC Coverage | Level |
|---|---|---|---|---|---|---|---|---|
| **Events Management** | Restricted Information related to an event (e.g. published sensor data) | Automatic gather of this kind of data when an event occurs (e.g. a sensor publish a data, the data is gathered and stored within the platform) | Sensors or data automatically gathered from the field | Gathered that cannot be deleted by an organization (and should not) | N.A. | Article 6, 17 are covered<br>Article 12 is partially covered (events cannot be deleted or modified)<br>Article 25 is not covered | Article 4, 5, 6 are covered in [D5.5]<br>Article 9 is not covered | **LOW** |
| **Status Management** | Information related to an organization's activities and personnel | Each organization activity update and personnel position is shared with all the other organizations in order to have a common operational picture of resources from the field. | The DESTRIERO platform internal repository | Each organization has the control on the published information | N.A. | Article 6, 12, 17 are covered<br>Article 25 is not covered | Article 4, 5, 6 are covered in [D5.5]<br>Article 9 is not covered | **MEDIUM** |

| Service | Sensitive Data | Data acquisition process | Source | Access, Correction, Deletion | Personal Information Notice | 95/46/EC Coverage | 2002/58/EC Coverage | Level |
|---|---|---|---|---|---|---|---|---|
| **Geographic Information** | Satellite imagery and map data | All the data is acquired through a third party system provided by EGEOS (WebGIS) and displayed through the DESTRIERO HMI. | The WebGIS Third Party System | No, users have no control on the satellite imagery or maps | N.A. | Article 6, 12, 17 are covered<br>Article 25 is not covered | Article 4, 5, 6 are covered in [D5.5]<br>Article 9 is not covered | MEDIUM |

**Table 2 - Data Protection and Privacy Issue for the DESTRIERO Methodology layer service**

## 3.3 Identification and analysis of legal requirements related to identified issues

In the previous chapter we have identified and analysed sources of potential ethical issues related with DESTRIERO and described the solutions adopted to manage them and guarantee the respect of the applicable international, EU and national law.

In this chapter we would like to provide recommendations that will help the consortium to identify early other possible ethical issues and deal with them in the proper way.

As we have seen, in DESTRIERO there are two separate areas that can be potential sources of ethical issues:

1) The project itself, since it requires interaction with, and occasionally collection of personal data from, external end users during the research activities and with the general public in dissemination.

2) The DESTRIERO platform: a tool for damage and needs assessment in post crisis situation, whose value proposition is based on data and information shared across organisations and systems.

Regarding ethical issues in research, European Commission provides useful guidelines **Errore. L'origine riferimento non è stata trovata.** and **Errore. L'origine riferimento non è stata trovata.** to identify and deal correctly with any ethics issues that may arise from it. In fact, this could happen in many areas of research, besides the obvious (related with health, animals, religion, gender etc) and the consortia must deal with them to protect end users, that voluntarily choose collaborate with projects, and protect themselves too.

In the questionnaire for self-assessment included in **Errore. L'origine riferimento non è stata trovata.** the only potential ethical issues in DESTRIERO research activities are related with personal data that, as described in chapter **Errore. L'origine riferimento non è stata trovata.**, are being dealt in a proper and legal way.

However it is important to endorse a series of recommendations to be kept into account, when approaching third parties to collect personal data. According to the current regulation we are required to:

- Provide details on the procedures for data collection, storage, protection, retention, transfer, destruction or re-use, methods of storage and exchange, data structure and preservation, data-merging or exchange plan.
- Provide details on our data safety procedures (protective measures to avoid unforeseen, usage or disclosure, including mosaic effect, i.e. obtaining identification by merging multiple sources).
- Confirm that informed consent has been obtained.

In case the scope of the activities involve further processing of previously collected personal data:

- Provide details on methods used for tracking or observing participants.
- Provide details on the database used or of the source of the data.

- Provide details on the procedures for data processing.
- Provide details on data safety procedures (protective measures to avoid unforeseen, usage or disclosure, including mosaic effect, i.e. obtaining identification by merging multiple sources).
- Confirm that data is openly and publicly accessible or that consent for secondary use has been obtained (and details on how this consent was obtained (automatic opt in, etc.)).
- Confirm permissions by the owner/manager of the data sets.

It is also important to remind that third parties or other project consortia we get in contact with have the same obligations toward us and we have the rights to ask for the details regarding our how data we provide are dealt, stored and processed.

Regarding the potential ethical issues related with the use of the DESTRIERO platform, there are two aspects that deserve special attention: **Dual use** (results and technologies that has the potential also for military applications) and **Misuse** (results and technologies that could potentially be misused).

The DESTRIERO tool, in its intention, addresses the needs of NGO or civilian forces in recovery and reconstruction operations, however in situations of high seriousness the deployment of military forces can be required and the access to the functionalities of DESTRIERO could be requested. Moreover DESTRIERO will be able to deal with data related with CBRN contamination that could be potentially misused.

Some recommendations should be considered in these cases:

- Provide explanations on the exclusive civilian focus of the research and its results.
- Justify inclusion of military partners or military technologies (i.e. explain how they relate to civilian applications, see for example **Errore. L'origine riferimento non è stata trovata.** where we propose the use of data model originally developed for military scope )
- Consult details on the legal requirements applicable on the use of biological-, chemical-, nuclear/radiological-security sensitive materials and explosives.
- Provide details on the measures you intend to take to prevent abuse (including training of personnel)

Keeping into account the scope of the project it is unlikely that the DESTRIERO consortium would be required to solve these issues during the lifetime of the project, however they may arise in the medium or long term and information to deal with them should be included in the support documentation delivered with the final product.

Finally, a general recommendation is to seek advice as soon as it is needed (from expert colleagues, ethics departments, relevant managers, ethics committees, ethics advisors, data protection officers, etc) to get the necessary information targeted at specific needs and legal requirements that must be addressed.

# 4 CONCLUSIONS AND RECOMMENDATIONS

In the European Union, privacy and data protection standards include the respect of EU Charter of Fundamental Human Rights and of the EU Data Protection Directive.

The sharing of personal data will be subject to relevant EU standards (e.g. data transfer only to countries able to ensure adequate levels of data protection).

Technologies that are planned to be used within the project will satisfy all the relevant laws and ethical regulations. Especially privacy and data security are in the centre of attention.

The project consortium commits itself to carry out all research activities in strict conformity with EU and national legislation and regulations, and to comply with the Charter of Fundamental Rights (2000) of the EU in respect to the citizen's dignity, freedom, equality, rights, and justice.

**According to the collected feedbacks from End Users**, the level of access to particular data and features should be differenced by users' role. It is recommended to establish **different levels of access**. It is also recommended a **user authentication mechanisms**, which would protect data from unauthorised access.

**According to EU legislation**, Article 9 *(Location data other than traffic data)* of EU Directive 2002/58/EC results not to be covered at the moment in DESTRIERO: it is recommended to **make location data to be transferred anonymous or to transmit location data with the consent of the users or subscribers to the service**.

**According to EU legislation**, Article 25 of EU Directive 1995/46/EC results not to be covered at the moment in DESTRIERO: it is recommended **not to transfer personal data to third countries**.