This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 787061

Advanced Tools for fighting Online illegal trafficking

D3.1 - European data protection framework and ethical requirements analysis

WP number and title	WP3 – Social, Ethical, Legal and Privacy issues of online sources analysis
Lead Beneficiary	IIP
Contributor(s)	ENG, CERTH
Deliverable type	Report
Planned delivery date	30/09/2018
Last Update	01/10/2018
Dissemination level	PU

Disclaimer

The ANITA Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Engineering Ingegneria Informatica	ENG	IND	IT
2	Centre for Research and Technology Hellas CERTH – ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	RTO	GR
3	Centro Ricerche e Studi su Sicurezza e Criminalità	RISSC	RTO	IT
4	Expert System S.p.A.	EXPSYS	SME	IT
5	AIT Austrian Institute of Technology GMBH	AIT	RTO	AT
6	Fundacio Institut de BioEnginyeria de Catalunya	IBEC	RTO	ES
7	Istituto Italiano per la Privacy	IIP	NPO	IT
8	SYSTRAN SA	SYSTRAN	SME	FR
9	Stichting Katholieke Universiteit Brabant	TIU-JADS	RTO	NL
10	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
11	Belgian Road Safety Institute	ISBR	RTO	BE
Law Enforcement Agencies (LEAs)				
12	Provincial Police Headquarters in Gdansk	KWPG	USER	PL
13	Academy of Criminalistic and Police Studies – Kriminalisticko-Policijska Akademija	AoC	USER	RS
14	Home Office CAST	CAST	USER	UK
15	National Police of the Netherlands	NPN	USER	NL
16	General Directorate Combating Organized Crime, Ministry of Interior	GDCOC	USER	BG
17	Local Police Voorkempen	LPV	USER	BE

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V0.1	01/06/2018	Draft	IIP	First draft
V0.2	1/08/2018	Draft	IIP	First draft integration with requirements tables
V0.3	18/09/2018	Completed version	IIP	Version ready for peer review
V0.4	24/09/2018	Reviewed version	ENG, RISSC	Peer reviewed version
V0.5	27/09/2018	Reviewed version	CERTH, DITSS	Peer reviewed version
V1.0	28/09/2018	Final version	IIP	Final
V1.1	01/10/2018	SAB review	Security Advisory Board (SAB)	Version reviewed by SAB
V1.2	01/10/2018	Final frozen	ENG	Version ready to be submitted

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
AAA	Authentication and authorization
CFREU	Charter of Fundamental Rights of the European Union
CoE	Council of Europe
CFREU	Charter of Fundamental Rights of the European Union
DBS	Database and Server
DM	Data Management
DoW	Description of Work
DP	Data Protection
DPAs	Data Protection Authorities
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEA	European Economic Area
EC	European Commission
ECHR	European Convention on Human Rights
EU	European Union
ER	Ethical requirements
FR	Functional requirements
GA	Grant Agreement
GDPR	General Data Protection Regulation
GR	General requirements
HTTPS	Hypertext Transfer Protocol Secure
I	Interoperability
ICT	Information and Communication Technologies
ID	Identifier
IP	Internet Protocol

IT	Information technology
LR	Legal requirements
LSPI	Legal, security and privacy issues
OR	Other requirements
OS	Operating system
PC	Privacy concerns
PMs	Person Months
PR	Privacy
QoS	Quality of service
R	Reliability
R&D	Research and development
SC	Scalability
SE	Security
SMS	Short Message Service
SOTA (or SoA)	State of the art
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
TLS	Transport Layer Security
Tor	The onion router
TR	Technical requirements
U	Usability
UN	United Nations
URL	Uniform resource locator
US	United States
VPN	Virtual private network
WP	Work package
WWW	World wide web

Table of Contents

List of Tables

Executive Summary

This deliverable D3.1 is the first deliverable from Work Package 3. The goal of Work Package 3 is to identify and tackle all potential legal and ethical issues of the project and its tools. So as to deal with the highlighted challenges, the following specific objectives are targeted: to evaluate data protection issues and impacts on the project with regard to the processing of personal data pursuant Regulation UE 2016/679 (General Data Protection Regulation) and Directive UE 2016/680; to evaluate the Cybersecurity Strategy for the European Union (e.g. NIS Directive) and European Union Agency for Network and Information Security activities; to define the cooperation between the Consortium and LEAs; to carry out an impact assessment concerning the possible ethical and legal risks for researchers involved in the project, in light of the likely sensitiveness and possible side effects of the envisaged research activity in dark web; to evaluate the impacts of the project on human rights with regard on how users make use of dark web, also for non-criminal and legitimate reasons and activities and evaluation of measures that might be taken to prevent abuses; to evaluate possible ethical issues that may arise in connection to potential misuse of the tools employed by the project made by governments affected by a high level of corruption or other potential issues.

Therefore, the following sections identify and analyse **ANITA requirements** from different angles, including:

- **Legal requirements** premised on personal data protection and data ownership, with a focus on European law;
- **Ethical requirements** designed to ensure rights, freedoms and societal compliance;
- **Technical requirements** relating to platform scalability, efficiency, reliability, and security.

From this perspective, developing these legal, ethical and technical requirements will **provide a common vision and shared understanding of underlying concepts throughout the entire ANITA project, to support the architecture design and the subsequent work of the other WPs, and integrate an ethics/data protection by design and by default approach**.

The current deliverable aims at providing a description of the work carried out in task T3.1, providing a complete overview of the identified requirements. To this aim, the report will primarily outline the relevant framework with regards to:

- Data protection legal obligations related to privacy risks (Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data; the General Data Protection Regulation (GDPR);
- the ethical principles constituted in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and all other applicable international, EU and national legislation in order to ensure an end-user acceptance and ethics compliance;
- Best practices and key features for the system and its processes, such as accountability, privacy impact assessment, risk minimization etc., taking into account the General Data Protection Regulation and the LEAs tasks in fighting and fighting criminals/terrorists in order to rebalance the traditional clash between privacy and security.

Introduction

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 right 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".

Article 8 of the *Charter of Fundamental Rights of the European Union (CFREU)*[1] binds the protection of personal data to a set of rights and principles for personal data processing, such as the specific purposes and consent of the person concerned, without differentiating between data held in the public or private sector. The aim of Art.8 *CFREU* is to guarantee data protection as a fundamental right, protecting individuals without impeding the free flow of information, via the legal certainty given to the data subject.

While the public may conflate data protection and privacy, there is an important distinction to be drawn between data protection and privacy. This lies in the fact that privacy is identified as the right of everyone *"to respect for his or her private and family life, home and communications*". In that sense, Art.7 *CFREU*[2] and Article 8 of the *European Convention on Human Rights (ECHR)*[3] protect an individual's private sphere. Art.8 *ECHR* specifies that this protection is subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society". In particular, Art.8 *ECHR* establishes that: *"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 means that privacy covers issues relating to the protection of an individual's personal space, so a possible interference must have a legal basis, having to be "in accordance with law".

Unlike the privacy right, which is a negative right – the right to be free of the "*interference by a public authority*" – the data protection right organises and controls the way personal data are processed, also covering the freedom of expression and the free flow of information. In effect, privacy concerns issues related to the protection of an individual's personal space (private communication, protection of family life, private home etc.). Data protection undoubtedly has a privacy dimension, but its scope is not just to protect the privacy of the data subject, but also to ensure an individual's ability to control information about him/her, guaranteeing fundamental rights such as freedom of expression, right to access,

---

[1] "*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 right 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.*", Article 8, Charter of Fundamental Rights of the European Union, 2012/C 326/02, in eur-lex.europa.eu.

[2] "Everyone has the right to respect for his or her private and family life, home and communications.", Article 7, Charter of Fundamental Rights of the European Union, 2012/C 326/02, in eur-lex.europa.eu.

[3] "*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.*" European Convention on Human Rights, Council of Europe, Rome, 4.XI.1950, in http://www.echr.coe.int/Documents/Convention_ENG.pdf.

modification, rectification or deletion, to know which data is stored about them and to avoid unnecessary data disclosure.

Several international treaties refer to privacy and data protection, binding the ratifying States to their obligations. The *Universal Declaration of Human Rights*, adopted by the UN General Assembly in 1948, states at Article 12: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".* The same disposition is provided in the *International Covenant on Civil and Political Rights* (1966, Art. 17[4]), the *Convention on the Rights of the Child* (1989, Art. 16[5]), the *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families* (1990, Art. 14[6]) and the *Convention on the Rights of Persons with Disabilities*, (2006, Art. 22[7]).

As regards data protection, the Organization for Economic Cooperation and Development (OECD) in its *Recommendation of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data* (1980, updated in 2013) addresses issues of personal data, purposes of collection, data disclosure and data subject right "*to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data*".

For the purposes of this Deliverable, we will mainly focus on data protection, although privacy protection will also be addressed, *where relevant*. Particularly, ANITA does not involve single human beings but focuses on the monitoring of illegal activities and of anonymous groups only. In fact, one of the main features of the dark web is the anonymity, which prevent the identification of the users. However, even if the identifiability (and the identity) of people is not a goal of the project, in case of incidental personal data collection, the Consortium will erase immediately any reference to an identified or identifiable person, excluding these data from the research. This process will be applied in personal data undesired collection only, because ANITA will not involve single human beings but the monitoring of anonymous groups only.

However, what ANITA will do for its end-users (LEAs) is to **realize a flexible system, with different settings based on three levels:**

- **The phase of the project (design, implementation, pilot, final product);**
- **The desired purposes (singling out of traffickers, criminal group monitoring) of the LEAs;**
- **The authorization of the LEAs officers – based on authentication measures, which will allow to give different kinds of usage permission.**

---

[4] "*1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks*", in *www.ohchr.org*.

[5] "*1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation. 2. The child has the right to the protection of the law against such interference or attacks*", in *www.ohchr.org*.

[6] "*No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks*", in *www.ohchr.org*.

[7] "*1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks. 2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others*", in *www.un.org*.

So, **the identifiability (and the identity) of suspected traffickers could be a goal of the final product, based on the LEAs investigation needs**. That is why D3.1 analyses:

- European norms on privacy and data protection, guaranteeing a lawful and accountable behaviour in order to comply with these norms, applying the accountability principle in order to give the Controller (i.e. the Consortium during the research phase in case of incidental personal data collection and the LEAs when using the final product) the responsibility and ability to demonstrate compliance with the **General Data Protection Regulation (hereinafter, "GDPR" or "Regulation") (Regulation (EU) 2016/679) and the Directive (EU) 2016/680 (hereinafter, "the Directive")**;
- Ethical issues as covered by European fundamental rights and freedoms that are associated with the ANITA objectives. Ethical norms are derived by the CFREU, in order to develop a fair decision-making process in designing project tools. **This report starts from the fundamental rights of the human beings to identify how rights, freedoms, privacy and data protection can be guaranteed also when fighting online illegal trafficking.**

By building an ethics and data protection by design approach, and combining ethical and legal issues with technical requirements, this Deliverable explores the balancing between non-discrimination, human dignity, public security and data protection - so as to create a set of technical and legal requirements guiding ANITA tools development.

1 Privacy and personal data protection within ANITA

This chapter analyses legal issues in terms of privacy and personal data protection, in order to develop a data protection by-design and by-default[8] approach to ANITA tools development.

It is paramount to underline that ANITA will design and develop a knowledge-based user-centered investigation system for analyzing online and offline contents for fighting illegal trafficking of drugs, counterfeit medicines, NPS and firearms.

In this sense, ANITA's "*end-users*" are the LEAs and they should not be confused with the "*users of the dark web*". The latter can be defined as potential "*data subjects*" in case of the identification (either incidental by the Consortium during the research phase or voluntary by the LEAs after the final product creation), being also the subjects that will be protected by GDPR rights (see Chapter 1) and ethical principles (see Chapter 2).

On the contrary, LEAs can be seen as "*data controllers*", so they are subject to obligations and duties established by the GDPR and Directive (EU) 2016/680, as described in Paragraph 1.1 and 1.2.

What ANITA will do for its end-users (LEAs) is to realize a flexible system, with different settings based on three levels:

- The phase of the project (design, implementation, pilot, final product);
- The desired purposes (singling out of traffickers, criminal group monitoring) of the LEAs
- The authorization of the LEAs officers – based on authentication measures, which will allow to give different kind of usage permission.

So, from the one hand, considering that the identifiability (and the identity) of data subjects is not a goal of ANITA project, personal data could be incidentally collected during the research phase, when analyzing online and offline contents during the tools development. In this case, the Consortium has to apply all the rules set by the GDPR.
On the other hand, the final ANITA platform/prototype will allow LEAs to gather personal data and process them for purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and this kind of processing is ruled by Directive (EU) 2016/680.

ANITA will not involve single individuals during the demonstration phase. In concrete, the system will be developed and integrated based on the direct involvement of the end-users (LEAs), in order the correctly address their needs, while the demonstration will be executed directly by the end-users (LEAs), in relevant secure LEA environments/premises.

Returning to the principles of data protection, they should apply to any information concerning an identified or identifiable natural person. In this sense, it is important to determine whether a natural person is identifiable. Recital 26 of the GDPR states that: "*account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural*

[8] Article 25, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).

person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable"[9].

As already mentioned, Art.8 *ECHR* stipulates the right to respect for private and family life, making clear that those rights are not absolute, because public authorities can interfere with Art.8 rights in certain circumstances. When the Council of Europe (CoE) adopted its *Convention .108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Council of Europe, 1981), it converged data protection and privacy in a single provision: "*The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*" (Art.1, *Convention n.108*)[10].

Through the *CFREU* (2000) and the *Treaty establishing a Constitution for Europe* (2004), the European Union has adopted legal obligations on both privacy and data protection. The *CFREU* refers, in Art.7, to the right of everyone "*to respect for his or her private and family life, home and communications*". Moreover, Art.8 *CFREU* refers specifically to "*Protection of personal data*", establishing main criteria for lawful processing, such as "*specified purposes*", the "*consent*", "*right of access*" and "*right to rectify*" and committing the control of the compliance with these rules to "*an independent authority*".

The *Lisbon Treaty*[11] (2007) states that the EU is founded upon the amended *Treaty on the European Union (TEU)*[12] and the *Treaty on the Functioning of the European Union (TFEU)*[13], which together provide a common legal framework for all the activities of the Union, including personal data protection.

Art.16 *TFEU* states that: "*Everyone has the right to the protection of personal data concerning them. 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* […]".

Processing of personal data by the EU institutions is dealt with by *Regulation 45/2001/EC of the European Parliament and of the Council 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*[14].

Processing of personal data for wider Member State activities which fall within the EU's competences are dealt with by the Regulation *(EU) 2016/679*, the *General Data Protection Regulation (GDPR)* and the *Privacy and Electronic Communications Directive (2002/58/EC, as amended by Directive 2009/136/EC)*.

Moreover, *Directive (EU) 2016/680* focuses on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. It means that GDPR

[9] Recital 26, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).

[10] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28.I.1981, in *www.coe.int*.

[11] *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, signed at Lisbon, 13 December 2007, in *eur-lex.europa.eu.*

[12] *Treaty on European Union and the Treaty on the Functioning of the European Union*, 2012/C 326/01, in *eur-lex.europa.eu.*

[13] Ibid.

[14] Regulation 45/2001/EC of the European Parliament and of the Council *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*, in *eur-lex.europa.eu.*

does not apply to processing activities for those purposes. However, it is paramount to remember that "*Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation*"[15].

For the purposes of this project Deliverable and in order to retrieve useful legal requirements for ANITA tools development, the following paragraphs will analyse principles and rules of the GDPR and Directive on processing of personal data by competent authorities. This approach will allow the Consortium to have a clear vision of the possible impacts on the rights of individuals using the dark web (for legal or illegal purposes) and establish a cooperation between the LEAs and the tools developers, defining solutions which will ensure legal and ethical standards through an Ethics-by-Design and Data Protection-by-Design strategy.

1.1 General Data Protection Regulation (GDPR)

The *Data Protection Directive (95/46/EC)* had extended the ideas of the *CoE Convention n.108*, referring to data processed by automated means and data contained in or intended to be part of non-automated filing systems to protect the right and freedom of persons by laying down guidelines on lawful data processing. With the introduction on the GDPR, some of the main points of Directive *95/46/EC* have been preserved, extending and introducing in parallel also new definitions, principles and obligation for the data controller/processor. Following Article 16 *TFEU*, which is the new legal basis for the adoption of data protection rules, the European Union legislator has adopted the GDPR. The aim of the Regulation is to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States, preventing disparities between Member States in terms of procedures and sanctions, harmonizing the Data protection law for all data controllers and data subjects based on EU. However, the Regulation also provides rules applicable to non-European data controllers if they process personal data of EU citizens.

The following list summarizes the core elements that must be taken into account when defining tools development and Consortium activities in research process (for the very compliance actions, please refer to Task 3.3 and Deliverable 3.4), in order to respect, since the design of the tools, data protection and privacy principles:

- **Lawfulness, fairness and transparency** of the data processing (Article 5(1)(a);
- **Data minimization**: the amount of data collected must be restricted to the minimum possible. These data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5(1)(c);
- **Purpose limitation:** data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), is not incompatible with the initial purposes (Article 5(1)(b);
- **Data quality and accuracy**: personal data must be "*accurate and, where necessary, kept up to date*" (Article 5(1)(d);
- **Storage limitation:** data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may

[15] Recital 19, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).

be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (Article 5(1)(e);

- **Integrity, confidentiality and security**: personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5(1)(f);
- **Accountability:** the controller shall be responsible for, and be able to demonstrate compliance with all the data protection principles provided for by Article 5(1) (Article 5(2);
- **Lawfulness of data processing**: Personal data may be processed only if the data subject has given his/her consent for one or more specific purposes or if processing is necessary: for the performance of a contract to which the data subject is party or; for compliance with a legal obligation to which the controller is subject or; in order to protect the vital interests of the data subject/another natural person or; for the performance of a task carried out in the public interest or; for the purposes of the legitimate interests pursued by the controller (Article 6);
- **Consent**: it should be freely given, specific, informed and unambiguous indication of the data subject's wishes about the data processing. The data subject has the right to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (Articles 7 and 4(11).
- **Special categories of personal data** (also called "sensitive personal data"): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is generally prohibited and can only be processed in exceptional circumstances (Article 9).

By analyzing the general elements of the Regulation, some of the most important provisions concern rights and obligations such as:

- **Information to be given to the data subject***:* the controller must provide the data subject from whom data are collected with information about the processing (e.g. the identity of the controller, the purposes of the processing, the legal basis for the processing, the recipients of the data, the existence of rights etc.) in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 12 and 13);
- The data subject's **right of access to data**: every data subject should have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed, and, where that is the case, access to the personal data and a number of information concerning the processing itself (Article 15);
- The **right to rectification** of inaccurate personal data concerning the data subject (Article 16);
- The **right to erasure ('right to be forgotten'):** under certain conditions, the data subject has the right to obtain from the controller the erasure of personal data concerning him/her without undue delay (Article 17);
- The **right to restriction of the processing:** the personal data are not subject to further processing operations and cannot be changed until the respect of principles or legal basis for processing are confirmed (Article 18);
- The **right to data portability**: under certain conditions, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another

controller without hindrance from the controller to which the personal data have been provided (Article 20);

- The **right to object to the processing of data**: the data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him/her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims (Article 21);
- **Automated individual decision-making, including profiling:** The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her, unless the processing is necessary for performance of a contract between the data subject and a data controller or; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent (Article 22);
- **Data protection-by-design,** that consist of the controller's implementation of appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles (e.g. data minimisation) in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects (Article 25(1);
- **Data protection-by-default**, that refers to the amount of data collected, retention period, extent of the processing and data accessibility. Essentially, the controller shall implement appropriate measures for ensuring that, "*by default, only personal data which are necessary for each specific purpose of the processing are processed*" (Article 25(2);
- **Designation of data processors:** where processing is to be carried out on behalf of a controller, the controller has to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures. Processing by a processor shall be governed by a written contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller (Article 28);
- **Records of processing activities:** each controller and processors shall maintain a written record of processing activities under its responsibility (Article 30);
- **Security of processing:** the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the existing and potential risk for personal data security, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. These technical and organizational measures can include: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (Article 32);
- **Data breaches** must be notified to the national supervisory authority not later than 72 hours after having become aware of it (with some exceptions accompanying the notification with the reasons for the delay) but also to the data subject without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (Articles 33-34);
- **Data protection impact assessment (DPIA)**, that must be carried out by the data controller "*where a type of processing in particular using new technologies, and taking into account the nature, scope,*

context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons", in order to maintain security and to guarantee the accountability (Article 35(1);

- **Prior consultation with the supervisory authority:** if the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller must consult the supervisory authority prior to processing (Article 36(1);
- **Data protection officer designation**, that has to monitor the compliance of the controller (or processor) with European and Member States data protection provisions. As underlined in Deliverable 12.2, when the processing is carried out by a public authority or body (except for courts acting in their judicial capacity) there is the obligation to have a Data Protection Officer. As the LEAs of the Consortium are "public authorities" in charge of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, they fall under art. 37(1)(a) of the GDPR that applies to processing "*carried out by a public authority or body*";
- **Data transfer** to third countries or to international organisations may take place on the basis of: an adequacy decision by the European Commission[16]; or, in the absence of such an adequacy decision, where the controller or processor provides appropriate safeguards, including enforceable rights and legal remedies for the data subject[17]. As analysed in D12.3, the ANITA consortium is composed of seventeen partners, one of them being an extra-European country: AoC, from Serbia. As stated in the Grant Agreement, AoC is the leader of Task 11.4 – Training activities, and, based on the aims of this task, AoC will organise training activities of officers of different LEAs and other relevant stakeholders, in order to equip them with comprehensive knowledge and effective skills to recognize and address illegal trafficking activities and to facilitate cooperation among LEAs. Training activities will be realised in the form of workshops, webinars, professional courses and face-to-face meetings, at individual-level, institutional-level and societal-level. In order to achieve the above aims of the task, AoC will be requested to access the personal data of the officers who are employees of the ANITA end-user LEA organisations that are/will be part of the ANITA User Community, which is managed by DITSS (User Community Manager). Therefore, a transfer of personal data from EU (Netherlands) to a third country (Serbia) will take place. As, so far, there is no adequacy decision by the European Commission on Serbia, the Consortium will use European Commission standard data protection clauses which are a proof of adequate data protection standards. Due to the relationship between DITSS and AoC within the ANITA project, they are both considered data controllers, therefore it will be used the controller-to-controller standard clauses (for further details see D12.3).

Article 29 of the Data Protection Directive established the ***Data Protection Working Party (Art.29 WP) – now called by the GDPR "European Data Protection Board" –*** that provides the European Commission with independent advice on data protection matters, helping in the development of harmonised policies for data protection in EU[18].

For the purposes of this report, we have analyzed some important opinions related to:

[16] General Data Protection Regulation, Art. 45

[17] General Data Protection Regulation, Art. 46

[18] For further details see *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*.

- The concept of personal data (*Opinion 4/2007*) "*to come to a common understanding of the concept of personal data*"[19];
- The definition of consent (*Opinion 15/2011*) to provide "*examples of valid and invalid consent, focusing on its key elements such as the meaning of "indication", "freely given", "specific", "unambiguous", "explicit", "informed" etc."*[20];
- Data protection issues related to the prevention of money laundering and terrorist financing (Opinion 14/2011)[21];
- Purposes limitation (*Opinion 3/2013*), to set "*limits on how data controllers are able to use their data while also offering some degree of flexibility for data controllers*"[22];
- The personal data breach notification (*Opinion 3/2014*) to help controllers "*to decide whether to notify data subjects in case of a "personal data breach*", considering the existing obligation of providers of electronic communications[23];
- Necessity and proportionality concepts and data protection within the law enforcement sector (*Opinion 01/2014*)[24];
- Anonymization techniques (*Opinion 5/2014*), to analyse "*the effectiveness and limits of existing anonymization techniques against the EU legal background of data protection*" and to provide "*recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them*" in order to help "*to choose how to design an adequate anonymization process in a given context*"[25];
- The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Opinion 03/2015)[26];

[19] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data,* Adopted on 20 June 2007, in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*.

[20] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent,* Adopted on 13 July 2011, in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*.

[21] Article 29 Data Protection Working Party, *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, Adopted on 13 June 2011, in http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf.

[22] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation,* Adopted on 2 April 2013, in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*.

[23] Article 29 Data Protection Working Party, *Opinion 03/2014 on Personal Data Breach Notification,* Adopted on 25 March 2014, in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*.

[24] Article 29 Data Protection Working party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, Adopted on 27 February 2014, in http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

[25] Article 29 Data Protection Working Party, *Opinion 5/2014 on anonymization techniques,* Adopted on 10 April 2014, in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*.

[26] Article 29 Data Protection Working Party, *Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, Adopted on 1 December 2015, in http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf.

1.2 Directive (EU) 2016/680

Considering that ANITA's "***end-users***" are the LEAs, which also can be defined as "data controllers", Directive (EU) 2016/680 establish a set of rules and principles to be applied to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in order to protect natural persons which can be identified in "dark web users". So, even if the GDPR constitutes the legal background for the data processing, there are some specific duties and norms for data processed by competent authorities as the LEAs.

As mentioned before, the identifiability (and the identity) of people is not a goal of the ANITA project and, thanks to the anonymity of the dark web, ANITA will monitor anonymous groups only. However, ANITA aims to realize a flexible ANITA prototype system, with different settings and its tools include the possibility to collect personal data of suspected traffickers, which must be processed in compliance with the GDPR and Directive principles. Under the new Directive, everyone's personal data must be processed lawfully, fairly, and only for a specific purpose, a purpose that is always linked to the fight against crime. The Directive ensures that personal data processing across the EU complies with the principles of legality, proportionality, and necessity, with appropriate safeguards for individuals. It also ensures completely independent supervision by national data protection authorities and effective judicial remedies.

The following list summarizes the core elements that must be taken into account when defining tools development and Consortium activities in research process (for the very compliance actions, please refer to Task 3.3 and Deliverable 3.4), in order to respect, since the design of the tools, data protection and privacy obligations/principles related to the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties as stated in Directive (EU) 680/2016:

- **Competent authority**. It means: (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Article 3(7).
- **Time-limits for storage and review.** Even if the data protection principles are the ones established by the GDPR, there is a special provision about appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. The competent authority must adopt procedural measures which ensure that those time limits are observed (Article 5).
- **Distinction between different categories of data subject.** There are four categories of data subjects affected by the Directive: (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; (b) persons convicted of a criminal offence; (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b) (Article 6). As mentioned before, ANITA research is not focused on personal data collection, but its tools (under certain conditions, such as LEAs officers authorization mechanism) could carry the LEA to the identification of suspected traffickers.
- **Lawfulness of processing.** A competent authority can process personal data only for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and these

purposes must be based on Union or Member State law. It also means that personal data collected by competent authorities for the above-mentioned purposes shall not be processed for other purposes unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes (including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes), Regulation (EU) 2016/679 shall apply (Articles 8-9).

- **Accountability.** Also in case of a processing carried out by a competent authority, the controller (i.e. LEA) shall be responsible for, and be able to demonstrate compliance with all the data protection principles provided for by Article 4 of the Directive, implementing appropriate technical and organisational measures. For example, as stated in Article 19, where proportionate in relation to the processing activities, these measures might include the implementation of appropriate data protection policies by the controller.
- **Processing of special categories of personal data.** The general prohibition of the GDPR about sensitive data processing is substituted by a general authorization for LEAs, but only where strictly necessary and with appropriate safeguards for the rights and freedoms of the data subject. Moreover, in order to avoid any discretional judgement made by the LEA, the processing of personal data must be based on a Union or Member State law; or to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject (Article 10). This kind of setting could be particularly relevant in case of monitoring of religion-based terrorism groups and in preventing attacks made by them.
- **Data protection by design and by default.** These two principles (Article 20 of the Directive) recall Article 25 of the GDPR.
- **Designation of data processors:** where processing is to be carried out on behalf of a controller, the controller has to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures. Processing by a processor shall be governed by a written contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller (Article 22);
- **Records of processing activities:** each controller and processors shall maintain a written record of processing activities under its responsibility, including, where applicable, the use of profiling and an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended (Article 24);
- **Logging.** Under Directive (EU) 2016/680, the controller and processor must keep logs for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. The logs are planned only for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings (Article 25)

By analyzing the general elements of the Directive, some of the most important provisions concern rights and obligations such as:

- **Automated individual decision-making.** Unless authorised by Union or Member State law to which the controller (LEA) is subject and which provides appropriate safeguards for the rights and freedoms of the data subject (e.g. obtain human intervention on the part of the processing), controller decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is prohibited. The same approach is followed for

decisions based on special categories of personal data, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place, in order to avoid discrimination against natural persons on the basis of special categories of personal data) (Article 11).

- **Information to be made available or given to the data subject.** The controller has to make available to the data subject at least the following information: (a) the identity and the contact details of the controller; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended; (d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority; (e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject related to the legal basis for the processing, the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period; the categories of recipients of the personal data, including in third countries or international organisations; further information, in particular where the personal data are collected without the knowledge of the data subject. These legislative measures can be adopted to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others (Article 13).
- **Right of access by the data subject and its limitations.** In case of processing under Directive (UE) 2016/680, the right of access has quite the same characteristics of Article 15(1), GDPR. It means that every citizen in the EU has an equal right of access to their personal data and they always have the right to approach the police and criminal justice authorities directly and ask for access to their personal data. However, Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others. In the above-mentioned cases, the controller must inform the data subject, in writing, of any refusal or restriction of access and of the reasons for the refusal or the restriction, underlining the possibility for the data subject to lodge a complaint with a supervisory authority or seeking a judicial remedy (Articles 14-15).
- **Right to rectification or erasure of personal data and restriction of processing.** While the right to rectification is similar to the GDPR provisions, the right to erasure is linked to different factors: first of all, it has to be executed where processing infringes the principles of processing, the provisions about lawfulness of the processing and the special categories of personal data dispositions, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject. Secondly, instead of erasure, the controller shall restrict processing where: (a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or (b) the personal data must be maintained for the purposes of evidence. As for the right of access, the controller has to inform the data subject, in writing, of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. It is up to Member States to adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic

society with due regard for the fundamental rights and legitimate interests of the natural person concerned, for the same reasons pointed out in case of right of access limitation (Article 16).

- **Rights of the data subject in criminal investigations and proceedings.** Where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings, it is up to the Member States to decide how to deal with the exercise of the rights referred to in Articles 13, 14 and 16 according to the Member State law.
- **Data protection impact assessment (DPIA)**. It must be carried out by the data controller "*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*", in order to maintain security and to guarantee the accountability (Article 27);
- **Prior consultation of the supervisory authority.** The controller or processor has to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where: (a) a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or (b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects (Article 28);
- **Security of processing.** The security of the processing responds to the same criteria set by the GDPR. However, the Directive specifies that, in respect of automated processing, the controller and processor have to implement measures designed to: (a) deny unauthorised persons access to processing equipment used for processing ('equipment access control'); (b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control'); (c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control'); (d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control'); (e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control'); (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control'); (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control'); (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control'); (i) ensure that installed systems may, in the case of interruption, be restored ('recovery'); (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity') (Article 29);
- **Data breaches.** Must be notified to the national supervisory authority not later than 72 hours after having become aware of it (with some exceptions accompanying the notification with the reasons for the delay) but also to the data subject without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (Articles 30-31).

1.3 Soft regulation and best practices for the ANITA system and its processes

ANITA project's development depends not just on legal obligations, but also on other important features that involve the processes and platform. In this sense, a number of aspects that need to be handled in the frame of the project have been identified also considering the GDPR and technical basic conditions to guarantee system functionalities:

1. **Minors of age involvement limitation.** Children inclusion into the investigation tool activities must be avoided, excluding minors' data collection (if possible) or storage after accidental collection.

2. **Ethics by design approach.** In order to protect citizens' rights and freedoms, the whole platform design will embed ethical requirements in all of its technical and organisational measures and procedures, which is an integral part of the accountability of the system.
3. **Data protection impact assessment and ethical assessment.** As a fundamental part of data protection and ethics-by-design approach, the Consortium will carry out an assessment of the impact of imagined processing operations on the protection of personal data and ethical values, in order to identify and reduce the privacy risks and rights and freedoms infringements.
4. **Accountability in data protection and ethics.** The project is based on effective procedures to report, document and explain the measures implemented to comply with data privacy law and ethical requirements, in order to ensure the compliance with data protection legislation, CFREU and ECHR. The Consortium will guarantee a lawful and accountable data processing throughout the duration of the project, considering that the identifiability (and the identity) of dark web users is not a goal of the research phase and, thanks to the anonymity of the dark web, ANITA will monitor anonymous groups only. As for its very nature ANITA's tools will have a flexible system, with different settings based on also on the purposes of LEAs investigations (singling out, groups monitoring), the establishment of a Data Protection and Ethics Office will avoid the potential misuse of research results and final products, both from partners of the Consortium and from external malicious actors by monitoring the researcher actions, defining a procedure for incidental personal data collection, implementing ethics and privacy policy etc. Through the application of the accountability principle, by producing all the relative compliance documents (e.g. records of processing activities, processors designation, data breach procedures etc.) the Controller (i.e. the Consortium during the research phase in case of incidental personal data collection and the LEAs when using the final product) will be responsible for and be able to demonstrate compliance with the GDPR and Directive 680/2016.
5. **Risk minimization.** ANITA will take all the security measures that are appropriate for minimizing the risk that personal data may be destroyed, lost, accessed without authorization, or processed unlawfully or by moving away from the purposes for which the data was collected.
6. **Technical features.** In order to combine the tools development with legal and ethical requirements, general properties of the system that concern its openness and availability, but also its compliance with legal/ethical obligations will be monitored for all the duration of the project. The ANITA Consortium acknowledges that work that will be conducted within project involves the development of technologies and the creation of information that could potentially have substantial direct impact on the security of the LEAs and on personal data of individuals. That is why ANITA will ensure the opportunity to customize the system according to the LEAs requirements and taking care of the trust level to achieve for each deployment. Multiple security mechanisms and technologies will ensure protection from malevolent/criminal/terrorist abuse.
7. **Distinction between "data" in general and "personal data**". A data is a piece of information. A personal data is a piece of information related to an identified or identifiable individual.

2 Ethical issues

This chapter analyses ethical issues in order to identify, from a normative perspective, the central elements and requirements that present a necessary condition for building trustworthy tools, eliminating any risks that could have a negative impact on the individuals' rights and freedoms, or that could adversely affect the environment.

In this sense, ethical requirements will be built on the ethical principles constituted in the Charter of Fundamental Rights of the European Union (CFREU) and the European Convention on Human Rights (ECHR) and all other applicable international and EU legislations.

This approach will allow the Consortium to have a clear vision of the possible impacts on the rights of individuals using the dark web (for legal or illegal purposes), ensuring tools ethical standards through an Ethics-by-Design strategy.

Particularly, ANITA will aim to ensure respect for people and human dignity, fair distribution of research benefits and burden and protecting the values, rights and interests of the research participants. Even if ANITA does not involve single human being but focuses on the monitoring of illegal activities and of anonymous groups only, the research results have the potential to be misused because the technologies developed by the ANITA consortium could have a severe negative impact on human right standards if they are misapplied.

In order to prevent any (intentional or unintentional) bias existing ex ante, prior to the design and development of the system, the designer's values or the values of end-users (LEAs) should be guided by common principles to be embedded into the system.

2.1 CFREU and ECHR rights and principles

In the EU legal environment and in all recitals of EU norms, one of the main constraints is to balance security and fundamental rights. Online security can only be sound and effective if they are based on fundamental rights and freedoms and individuals' rights.

Article 52 of CFREU states that: "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*". The Charter provide safeguards for fundamental human rights which may be only interfered by legitimate law enforcement activities. In order to do so, there are three elements to be considered:

1) What precisely is the **national law** to be taken into consideration, analyzing to what extent it was accessible and cognizable. The interference must have some basis in domestic law and be compatible with the rule of law; and the law must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to regulate his or her conduct[27].
2) Furthermore, since only a **legitimate need** can limit the rights and freedoms of individuals, there should be an evaluation of proportionality of that restriction for the purpose set by the provision, considering whether this contrast was justifiable insomuch as necessary **in a democratic society**. To

[27] Article 29 Data Protection Working party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, Adopted on 27 February 2014, in http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

be in pursuit of a legitimate aim requires that an activity is carried out in pursuance of one of the aims set out in Art. 8(2) ECHR, e.g. the prevention or detection of disorder or crime, protection of the rights and freedoms of others etc[28].

3) The criterion of "**necessity**" should not be confused with an arbitrary judgment on the usefulness of the restriction because the interference must always respond to an urgent social need, be commensurate with the objective, and have adequate and relevant reasons[29].

In this sense, protecting fundamental rights, freedom of expression, personal data and privacy needs to cope with the security need, proportionating safety and human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. For cyberspace (e.g. surface web, deep web and also dark web) to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace while protecting against incidents, malicious activities and misuse[30].

As ANITA aims to develop advanced tools for fighting online illegal trafficking, this security purpose must be balanced with the following ethical pillars, established by the CFREU and ECHR:

- **Human dignity** (Article 1, CFREU) which includes respect for private and family life (Article 7, CFREU and 8, ECHR), protection of personal data (Article 8, CFREU), freedom of expression and information (Article 11, CFREU) which has to be interpreted as the right produce/publish/transmit/share data (active profile), but also to be able to be informed by those who prepare and transmit news of public interest (passive profile) and also to be able to access that news. Already if these three basic profiles are considered, it is clear that such freedom is also founded on the right to research information and sources and on guarantees of pluralism;
- **Equality and non-discrimination** which includes equality before the law (Article 20, CFREU) and prohibition of any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation (Article 21, CFREU), which is linked to the freedom of thought, conscience and religion (Article 10, CFREU);
- **Presumption of innocence and right of defence** (Article 48, CFREU) which guarantees that everyone who has been charged shall be presumed innocent until proved guilty according to law. Moreover, anyone who has been charged has the right of the defence.
- **Principles of legality and proportionality of criminal offences and penalties** (Article 49, CFREU) that excludes the possibility to declare someone guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national law or international law at the time when it was committed.

[28] Ibid.

[29] The Sunday Times v. The United Kingdom, No. 6538/74, §42, ECHR 1979 in hudoc.echr.coe.int.

[30] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 2.

3 Data protection and ethical requirements definition

The requirement definition process is a critical goal in systems development, since one generally accepted cause of a system failures is poor requirement identification. The process of determining requirements usually has three stages: (1) information gathering, (2) representation, and (3) verification *(Pitts & Browne, 2007)*[31]. The requirement engineer has to "dig" down and analyses all the useful sources (laws, opinions, studies, best practices etc.) in order to identify the elements that has to guide the system development from its design.

The chosen perspective for requirements identification is dual:

- On the one hand the locating perspective, applicable to legal issues, which assumes that the requirements are something that actually exist and merely have to be found. That perspective follows that requirements are stable and recognisable.
- On the other hand, the constructing view *(Imaz, 2006*[32]*; Sharp et al., 2007*[33]*)*, already experimented in successful European projects, can be applied to ethical issues. This approach includes creating something new by combining identified elements in new ways *(Imaz, 2006*[34]*)*, that can be very important when it comes to gather different interests (e.g. LEAs needs; citizens' rights and freedoms) starting from a common ethical sense derived by CFREU and ECHR.

Following both approaches, the requirements fulfilment will be monitored for the entire duration of the project through a Data and Ethics Control (Task 3.3) which will follow the requirements evolution. Hence, the majority of requirements presented in this deliverable are design principle oriented and based on the balancing between human values (rights and freedoms) and data protection law dispositions (obligations and duties for the controller, rights of data subjects).

3.1 Requirements design methodology

The first step will be to take inputs and expertise from the ANITA project members/individuals involved in the project, to develop the initial version of the system. This holds true for legal requirements as well; they have been extracted by the Consortium's legal experts, from a repository of applicable norms, and tailored to the project's platform and architecture by taking into consideration:

a) The discussions held within the Consortium, amongst legal and technical partners, starting from the project's kick-off meeting held in Rome in May 2018, and continued in subsequent telcos and emails exchanges;
b) The definition of the initial system's and architecture's features, which resulted in the identification of necessary technical and user requirements by the relevant partners, on which legal requirements were devised.

[31] Pitts, M.G., and Browne, G.J. (2007). Improving Requirements Elicitation: An Empirical Investigation of Procedural Prompts. *Information Systems Journal,* 17(1).

[32] Imaz, M. (2006). *Designing with Blends: Conceptual Foundations of Human-Computer Interaction and Software Engineering.* Cambridge, MA, USA: MIT Press.

[33] Sharp, H., Rogers, Y., and Preece, J. (2007). *Interaction Design: Beyond Human-Computer Interaction*. 2nd ed. Chichester: John Wiley & Sons Ltd.

[34] Imaz, M. (2006). *Designing with Blends: Conceptual Foundations of Human-Computer Interaction and Software Engineering.* Cambridge, MA, USA: MIT Press.

Clearly, the specific features of the multifaceted ANITA system and components cannot be entirely known in advance at the moment the requirements are drafted.

Two corrective measures can however be deployed, in order to prevent the risk of outdated or non-pertinent requirements:

- the first measure is ensuring a close interaction between partners with different expertise within the Consortium, in order for legal experts to be constantly aligned with technology's developments within the project and for technical experts to be fully instructed on the practical consequences of changes in the legal framework or in the technological environment considered.
- The second corrective measure consists of involvement of the LEA end-users into creation of the system; this exercise is part of WP4 and the test and demonstration of the ANITA tools prototype being part of WP10. End-users' feedback, concerning what are their expectations in terms of project's outcomes and system's functioning, will be considered for the whole duration of the project. During the co-creation phase, workshops and meetups feedback will be collected from the LEAs involved in the project.

3.2 Detailed requirements analysis

In this section an initial set of requirements was compiled. They indicate a property or a service of the system, which may be of interest either for the LEAs perspective or for the Consortium as a whole. Each requirement will be revised during the project, taking into account the development of the system and the suggestions of the research community. The whole work on requirements is reported in a table like the following:

Requirement title (ID)	…
Level of criticality	…
Definition and description	…
Complementary explanations	…

Table 1: Requirements table sample

Therefore, each requirement will have:

1. A title and an identification code. The latter comes from the category or subcategory to which the requirement belongs;
2. A level of criticality from 1 to 3. Requirements marked with:
    a. **Level 3** described as "critical" because they either stem from legal obligations directly applicable to the system and the project or they are necessary for the system to technically work in its basic functions;
    b. **Level 2** requirements are "important", which means that failure to implement them would result in a major malfunctioning of the system or increase the risk of legal non-compliance;
    c. **Level 1** requirements are those that functionally are "optional" and if embedded into the system, will align it with non-binding legal recommendation/s and ease the end-user's experience (optional).
3. A synthetic definition and description;
4. Some complementary explanations, which can further detail the presented requirement, its rationale and eventually refer to any relevant normative basis, etc.

3.3 Requirements classification

The requirements have been classified in five main categories:

- General requirements, which constitute the baseline requirements, horizontally applicable to all the functions and components of the system.
- Technical requirements extend the 'General Requirements' classification with requirements related to the system architecture and the characteristics of the overall platform.
- Legal requirements, referring to legal obligations whose respect must be ensured by the system and its components.
- Ethical requirements, meaning the requirements derived by ethical pillars described in this document.
- Other Requirements, encompassing the requirements not classified/classifiable under any of the above-mentioned categories.

Each category has been split in several subcategories:

General requirements (GR)

- Generic functional requirements (FR), grouping transversal requirements that shall be referred to all tools and enablers of the project;
- Authentication and authorization (AAA), identifying credentials and authorization profiles of data processors to access the system;
- Project configuration (PC), providing end-users with information about the project and rules for processing of personal data;
- Data management (DM), about the control on the collected data and permitting the system to respond to the incidental personal data collection;
- Database and servers (DBS).

Complementary Technical Requirements (TR)

- Reliability (R)
- Security (SE)
- Privacy (PR)

Legal requirements (LR), complying with all the legal data protection and privacy obligations from Consortium perspective (research phase) and LEAs one (final product usage);

Ethical requirements (ER), linked to the rights and freedoms of cyberspace users;

Other requirements (OR), to align as much as possible with the end-user needs and expectations pointed out in WP4.

3.4 Detailed requirements description and explanation

3.4.1 General requirements (GR)

3.4.1.1 Generic functional requirements (FR)

Requirement title (ID)	**Project data management plan** (GR_FR_01)
Level of criticality	3
Definition and description	The data management plan describes the data management life cycle for the data to be collected, processed and/or generated by ANITA.

Complementary explanations	The DMP will include information on: a) the handling of research data during & after the end of the project, b) what data will be collected, processed and/or generated, c) which methodology & standards will be applied, d) whether data will be shared/made open access and, e) how data will be curated & preserved (including after the end of the project).

Table 2: General requirements – Generic functional requirements – Project data management plan

Requirement title (ID)	**Data back-ups** (GR_FR_02)
Level of criticality	3
Definition and description	Back-up operations will be carried out periodically, so as to ensure the continuity of the system and prevent the loss of data.
Complementary explanations	ANITA will provide back-ups for each system's tools, in order to ensure the maintenance and the continuity of information and complete traceability of each activity.

Table 3: General requirements – Generic functional requirements – Data back-ups

3.4.1.2 Authentication and authorization (AAA)

Requirement title (ID)	**Authentication** (GR_AAA_01)
Level of criticality	3
Definition and description	Persons in charge of the processing, i.e. individuals acting on behalf of the data controller – ANITA consortium or LEAs agents – data processor and sub-processor, must have individual authentication credentials composed by a personal ID code and a secret password with at least eight characters; if this is not allowed, the password shall consist of the maximum permitted number of characters and it shall not contain any item that can be easily related to the person in charge of processing. It shall be also modified when it is first used as well as periodically, thereafter. Alternatively, these credentials shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing or in a biometric feature (possibly, in both cases, associated with either an ID code or a password).
Complementary explanations	The whole system will collect different types of data and it will be designed to ensure the privacy, rights and freedoms of the cyberspace users. In order to do this, person in charge of the processing will be authenticated and appropriately authorised to be able to use the system. Where necessary, strong authentication (e.g. double opt-in, biometric recognition, etc.) methods must be in place.

Table 4: General requirements – Authentication and authorization – Authentication

Requirement title (ID)	**De-activation of authentication credentials** (GR_AAA_02)
Level of criticality	2
Definition and description	Personal authentication credentials can be de-activated if they have not been used (except in case of technical authorization). The system will periodically check if more than six months elapsed since the last log in of each person in charge of the processing and, in this case, it disables the credentials. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data.
Complementary explanations	The objective is to guarantee that persons in charge of the processing are allowed to process personal data only if they are provided with authentication credentials. The credentials will be necessary for the appointed person to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.

Table 5: General requirements – Authentication and authorization – De-activation of authentication credentials

Requirement title (ID)	**Authorization** (GR_AAA_03)
Level of criticality	3
Definition and description	Before the start of the processing, it is necessary to enable access to the data that are needed to perform processing operations, setting out an authorization profile for each person/homogeneous set of persons in charge of the processing.
Complementary explanations	Authorization profiles for persons in charge of the processing must be set out and configured prior to start of the processing so as to their access only to the data that are necessary to perform processing operations. It shall be regularly verified, in accordance with the reporting periods, to check if the composition of the teams has changed and if the prerequisites for retaining the relevant authorization profiles still apply. Drawing up a list of persons in charge of the processing to identify categories of task and corresponding authorization profile.

Table 6: General requirements – Authentication and authorization – Authorization

3.4.1.3 Project configuration (PC)

Requirement title (ID)	**Information on tools usage** (GR_PC_01)
Level of criticality	3

Definition and description	Before the final product delivery, end-users (i.e. LEAs) will receive prior information about data processing rules and ethical standards, with a brief project purposes description.
Complementary explanations	It is necessary to provide to LEAs all the information about the whole system in order to make them informed before their usage of specific project tools.

Table 7: General requirements – Project configuration – Information on tools usage

3.4.1.4 Data management (DM)

Requirement title (ID)	**Incidental personal data collection** (GR_DM_01)
Level of criticality	3
Definition and description	During the research phase, in case of incidental personal data collection, the system enables the Consortium to delete them immediately or at the moment of the collection is discovered.
Complementary explanations	The idea, in case of incidental personal data collection, is that the Consortium will erase immediately any reference to an identified or identifiable person, excluding these data from the research. This process will be applied to personal data undesired collection only.

Table 8: General requirements – Data management – Incidental personal data collection

Requirement title (ID)	**Data management plan update** (GR_FR_01)
Level of criticality	3
Definition and description	The data management plan will be released at month 6 and updated at month 36 in order to describe the data management life cycle for the data to be collected, once the final product is ready.
Complementary explanations	The DMP update reports on final rules and practices about data management procedures that have been followed throughout the ANITA project. It will deal also with the generation of data for the Open Research Data Pilot, describing what data ANITA has generated and how these data are made available and managed.

Table 9: General requirements – Data management – Data management plan update

3.4.1.5 Database and servers (DBS)

Requirement title (ID)	**Data processors' obligations** (GR_DBS_02)
Level of criticality	3

Definition and description	ANITA data processors are the partners who will provide technical services to the Consortium (data controller) for the purpose of performing the project's activities. Data processors must be regularly designated and selected among entities that can ensure, on account of their experience, capabilities and reliability, compliance with the provisions in force applying to processing. Each data processor will take the necessary precautions to ensure the secrecy of credentials and operate fully complying with the data protection legislation in terms of data processing and security issues.
Complementary explanations	ANITA data processors are nominated in writing with a contract or legal act (see Bind the processor to the controller (LR_10) requirement), identifying the scope of the processing and the operations that are permitted. Each one of them will be provided with authentication credentials (see Authentication (GR_AAA_01) requirement) in order to complete the authentication procedure. Credentials could be deactivated (see De-activation of authentication credentials (GR_AAA_02) requirement).

Table 10: General requirements – Database and servers – Data processors' obligations

Requirement title (ID)	**Confidentiality** (GR_DBS _03)
Level of criticality	3
Definition and description	ANITA database and servers have to retain the confidentiality of the data during all operations.
Complementary explanations	ANITA database and servers will provide mechanisms to ensure the confidentiality of the stored data. SSL/TLS encryption will protect data in transit for the front-end operations and VPN connectivity for the internal transactions between the database and servers. Moreover, according to ANITA project, as incorporated in the Grant Agreement signed with the EC (paragraph 5.1.2, page 259) the Consortium will include "*Adoption of Secure Protocols for data communication against the risk of data breaches (e.g. https)*".

Table 11: General requirements – Database and servers – Confidentiality

Requirement title (ID)	**Role Based Access Control** (GR_DBS _04)
Level of criticality	3
Definition and description	ANITA database and servers should support Role-Based Access Controls to restrict access to authorized persons only.
Complementary explanations	Database and servers will provide different levels of access to developers, operators and administrators according to their responsibilities on a need

	to know basis. Detailed audit controls will be enforced to maintain a clear overview of the actions of all involved factors.

Table 12: General requirements – Database and servers – Role Based Access Control

Requirement title (ID)	**Business Continuity** (GR_DBS _05)
Level of criticality	2
Definition and description	Database and servers will be deployed in compliance with the Business Continuity plan to ensure the availability of ANITA services after unpredictable incidents and events.
Complementary explanations	Database and servers will be resilient utilizing replication and redundancy both in a physical and logical implementation. The replication procedure will also assure data integrity with multiple backup sites and mechanisms.

Table 13: General requirements – Database and servers – Business Continuity

3.4.2 Complementary technical requirements (TR)

3.4.2.1 Reliability (R)

Requirement title (ID)	**Reliability** (TR_R_01)
Level of criticality	2
Definition and description	ANITA system must operate in a trustworthy manner, producing always the same result after an input given in specific conditions. The standardization of outputs allows guaranteeing equality of treatment and non-discrimination of end-users (e.g., different operating systems will produce the same output). Reliability also concerns system failures that must be prevented and resolved through the adoption of specific measures, such as back-up procedures and disaster recovery plans.
Complementary explanations	The system reliability concerns ordinary situations but also those situations in which a system failure occurs. System administrators will be in the position to adopt technical remedies and to ensure the maintenance of the equality and non-discrimination of treatment of all users regardless to the state of the system.

Table 14: Complementary technical requirements – Reliability – Technical interoperability of system and services

3.4.2.2 Security (SE)

Requirement title (ID)	**Protection measures for interfaces** (TR_SE_01)

Level of criticality	3
Definition and description	The system must set a Governance Layer equipped by a customizable Access Control Module able to verify researchers, operators and administrators' permissions and monitoring all of their activities. Developers, operators and administrators can access to the system after a successful login based on username and password.
Complementary explanations	Security relates to the capability of the system to ensure that data is transmitted, stored, disclosed and processed in accordance with legal requirements and in combination with the guarantee of developers, operators and administrators' authentication and authorization to access system services, applying IP restrictions, administrator roles and privileges.

Table 15: Complementary technical requirements – Security – Protection measures for interfaces

Requirement title (ID)	**Registration and authentication of LEAs agents** (TR_SE_02)
Level of criticality	3
Definition and description	The system must permit that certain services are only accessible to end-users with a verified identity. In order to do so, the system must have a reserved area. Clearly, there will be open services for non-logged-in users, but, in general, there will be a reserved area for end-users, in which these subjects could enter their personal ID and password to log-in – obviously, there will be the possibility for both subjects to log-out.
Complementary explanations	As a part of Security requirement (TR_SE_01), the system must permit that certain services are only accessible to end-users with a verified identity and in a reserved area, in order to ensure that access to data stored and certain services offered are granted only to authorised users/SMEs.

Table 16: Complementary technical requirements – Security – Registration and authentication of LEAs officers

Requirement title (ID)	**Data integrity and confidentiality** (TR_SE_03)
Level of criticality	3
Definition and description	The system must ensure that the data stored and exchanged between LEAs agents and the system itself will not be accidentally modified during the storage/exchange or corrupted by a third non-authorised party. Moreover, the system must guarantee that said data are confidential and they are not disclosed to unauthorised persons.
Complementary explanations	Any person who has access to personal data must not modify or disclose them (see Security of data storage (FR_LR_08) and Bind the processor to

	the controller (FR_LR_10) requirements).

Table 17: Complementary technical requirements – Security – Data integrity and confidentiality

Requirement title (ID)	**Password and data encryption** (TR_SE_04)
Level of criticality	3
Definition and description	The system must guarantee that authentication passwords will not be read without applying the appropriate decoding algorithm. The same safeguard must be given to stored/transmitted data in order to ensure data confidentiality and integrity.
Complementary explanations	Data encryption will be applied to all personal and authentication data, in order to make end-users credentials and collected cyberspace users personal data encoded in non-readable format even if the stability of the system is compromised. This requirement goes hand in hand with Reliability requirement (NFR_TR_R_01).

Table 18: Complementary technical requirements – Security – Password and data encryption

Requirement title (ID)	**End-to-end security** (TR_SE_05)
Level of criticality	3
Definition and description	End-to-end security means “full lifecycle protection”.
Complementary explanations	End-to-end security is a paradigm of an interrupted protection of data traveling between two communicating parties without being intercepted or read by other parties. This requirement is linked to Confidentiality requirement (GR_DBS _03).

Table 19: Complementary technical requirements – Security – End-to-end security

3.4.2.3 Privacy (PR)

Requirement title (ID)	**Layered notice** (TR_PR_01)
Level of criticality	2
Definition and description	The system must provide different level of information, where the initial notice contains the minimum information required by the EU legal framework and further information is available through links to the whole privacy policy of the tool. Information can be provided to the registered end-users in a user friendly and comprehensible way, possibly by icons.
Complementary explanations	The Art. 29 WP sees benefits in the use of layered notices where the initial notice to the end-user contains the minimum information required by the EU legal framework and further information is available through links to the whole privacy policy (*Opinion 02/2013 on apps on smart devices*). This

	orientation will go hand in hand with the project objectives so as to give to end-users the capability understand the system (see Information on tools usage requirement (GR_PC_01).

Table 20: Complementary technical requirements – Privacy – Layered notice

Requirement title (ID)	**Privacy and ethics by design approach to data processing** (TR_PR_02)
Level of criticality	3
Definition and description	Due to the nature of data stored in the system, which can also be personal data, the system itself must be secured against any threat of intrusion, violation, breach or alteration. Privacy must be a default setting. Moreover, privacy and ethical values must be embedded into the design, as an essential component of the system – see Accountability (LR_17) requirement.
Complementary explanations	In order to ensure the privacy and ethics by-design approach the system will use privacy friendly and ethical principles as default options. This position is clearly stated by Article 25 of GDPR and Article 20 of the Directive.

Table 21: Complementary technical requirements – Privacy – Privacy and ethics by design approach to data processing

3.4.3 Legal requirements (LR)

Requirement title (ID)	**Lawfulness of the processing** (LR_01)
Level of criticality	3
Definition and description	What ANITA will do for its end-users (LEAs) is to realize a flexible system, with different settings based on three levels: - The phase of the project (design, implementation, pilot, final product); - The desired purposes (singling out of traffickers, criminal group monitoring) of the LEAs - The authorization of the LEAs officers – based on authentication measures, which will allow to give different kind of usage permission. Consortium perspective: So, from the one hand, considering that the identifiability (and the identity) of data subjects is not a goal of ANITA, personal data could be incidentally collected during the research phase, when analysing online

	and offline contents and pre-existing datasets during the tools development. In this case, the Consortium has to apply all the rules set by the GDPR, taking into account the Incidental personal data collection (GR_DM_01) requirement. LEAs perspective: On the other hand, the final product will allow LEAs to gather personal data and process them for purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and this kind of processing is ruled by Directive (EU) 2016/680. ANITA will not involve single individuals during the demonstration phase. In concrete, the system will be developed and integrated based on the direct involvement of the end-users (LEAs), in order the correctly address their needs, while the demonstration will be executed directly by the end-users (LEAs), in relevant environments.
Complementary explanations	The lawfulness of processing carried out by the Consortium is based on different grounds, if compared with the lawfulness conditions of a data processing carried out by a competent authority. The latter can process personal data only for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and these purposes must be based on Union or Member State law. It also means that personal data collected by competent authorities for the above-mentioned purposes shall not be processed for other purposes unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes (including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes), Regulation (EU) 2016/679 shall apply (Articles 8-9 of the Directive). When it comes to the Consortium potential data processing, Article 6 of the GDPR is applicable: personal data may be processed only if the data subject has given his/her consent for one or more specific purposes or if processing is necessary: for the performance of a contract to which the data subject is party or; for compliance with a legal obligation to which the controller is subject or; in order to protect the vital interests of the data subject/another natural person or; for the performance of a task carried out in the public interest or; for the purposes of the legitimate interests pursued by the controller. However, ANITA does not involve single human beings but focuses on the monitoring of illegal activities and of anonymous groups only. In fact, one of the main features of the dark web is the anonymity, which prevents the identification of the users. In case of incidental personal data collection, the Consortium will erase

	immediately any reference to an identified or identifiable person, excluding these data from the research (see Incidental personal data collection (GR_DM_01) requirement).

Table 22: Legal requirements – Information to data subject

Requirement title (ID)	**Purpose limitation** (LR_02)
Level of criticality	3
Definition and description	ANITA will enable two different purposes of data processing which depend on the stage of the research: 1) Purposes of monitoring anonymous groups operating on the dark web, during the tools designing and implementation phase; 2) Purposes of the prevention, investigation, detection or prosecution of criminal offences through the final product offered to LEAs, which may include both the monitoring of anonymous groups and singling out the traffickers. Starting from this, ANITA's tools will process cyberspace users' personal data only for legitimate, specific and explicit purposes, determined at the time of collection of the data through two different and specific privacy policy: a) The one for the Consortium acting as data controller, that could incidentally collect personal data (see Incidental personal data collection (GR_DM_01) requirement) for the sole purposes of the project, namely to design and develop a novel knowledge-based user-centred investigation system for analyzing heterogeneous (text, audio, video, image) online (Surface Web, Deep Web, DarkNet) and offline content for fighting illegal trafficking of drugs, counterfeit medicines, NPS and firearms. b) The one for the LEAs that will act as data controllers after the release of the final product, choosing the type of investigation (monitoring of anonymous groups or singling out), based also on the authorization profile of the officer (see Authorization requirement (GR_AAA_03).
Complementary explanations	Purposes of the data processing will be well defined and comprehensible into the above-mentioned privacy policies. This requirement implements the purpose limitation principle set forth by Article 5(1)(b) of the GDPR and 4(1)(b) of the Directive. Having regards to the Consortium data processing, the Art. 29 WP has provided an in-depth analysis of this principle in its *Opinion 03/2013 on purpose limitation*, which will be taken into account. In fact, even if pre-

	existing data sets would be used during the project, this does not mean to involve secondary use of personal data, as the further processing of personal data for scientific research is not to be considered to be incompatible with the initial purpose (Article 5, 1(b) and 89, 1) of the GDPR). Data processing carried out by LEAs will be covered by the *Opinion 3/2015* of Art. 29 WP, which anticipates the contents of Recitals 11-12 of the Directive underlining that in order to ensure a consistent and high level of protection, "*the processing activities performed by the competent authorities for purposes not linked to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be clearly maintained under the scope of the Regulation*". Furthermore, purpose limitation and distinguishing between different categories of personal data lead to other considerations: "*Specific data or data on specific categories of data subjects might be necessary in certain criminal investigations. However, their further use should be limited and strictly conditioned, in particular where the relation between a person and a crime is not established (the collection of data on this person is related to a crime but they are not classified as suspects, victims and witnesses). More specifically, contrary to data relating to suspects or convicted persons, the further use of data relating to "non suspects" should be prohibited*".

Table 23: Legal requirements – Purpose limitation

Requirement title (ID)	**Data minimization** (LR_03)
Level of criticality	3
Definition and description	Collected data will be adequate, relevant and not excessive in relation to the purposes for which they are processed, in order to prevent unnecessary and potentially unlawful data processing.
Complementary explanations	The normative base of data minimization is Article 5(1)(c) of the GDPR, recalled also by Article 4(1)(c) of the Directive. In the *Opinion 3/2015* Art. 29 WP underlines that "*only the minimum amount of personal data should be processed to achieve the purpose set out; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not constitute personal data*". In the scope of the Directive, Art. 29 WP recalls Recommendation No. R(87)15 which states in principle 2.1 that "*the collection of personal data for police purposes should be limited to that which is necessary for the*

	prevention of a real danger or the prevention of a specific criminal offence".

Table 24: Legal requirements – Data minimization

Requirement title (ID)	**Data accuracy and updating** (LR_04)
Level of criticality	3
Definition and description	Data subjects', which are inaccurate or incomplete, having regard to the purposes for which they were collected or processed, will be erased or rectified.
Complementary explanations	The normative base of data accuracy and updating is Article 5(1)(d) of the GDPR and Article 4(1)(d) of the Directive.

Table 25: Legal requirements – Data accuracy and updating

Requirement title (ID)	**Data anonymization and pseudonymization** (LR_05)
Level of criticality	3
Definition and description	In order to limit the responsibilities of the ANITA Consortium acting as the data controller, ANITA must provide for technical and organizational measures to ensure, as much as possible, that data are irreversibly anonymised and aggregated, permitting identification of data subjects for no longer than is necessary. When anonymization is not possible or not desirable, pseudonymization should be set as the default option. This means that a code is attributed to each data subject and that the re-identification of users takes place only if strictly necessary to prevent frauds, misuse of the Services, damages to ANITA and any third parties, any other breach of relevant law and to defend a legal claim.
Complementary explanations	As stated before, ANITA will not involve single human beings but the monitoring of anonymous groups only. Moreover, the identifiability (and the identity) of people is not a goal of the project. However, in the exceptional cases of incidental collection of personal data, or collection of personal data of suspected traffickers, the personal data will be stored in a secured and isolated way that makes it impossible for the LEAs to access individual personal data. The end-users (LEAs) will only be able to see the overall information so as to prevent any risk of "singling out", "linkability" and "inference" of data. In fact, on the perspective of the Consortium, the data collected will be pseudonymised in order to be safe even in case of a breach in the security system. In the context of the dark web, which is well known for the anonymity it offers, is important to remember that, having regard to data protection

	principles in case of anonymization, the GDPR and Directive state that: "*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*". So, both the GDPR and Directive does not concern the processing of such anonymous information, including for statistical or research purposes (e.g. monitoring of anonymous groups in the dark web). Having regard to the pseudonymization, the GDPR, in Article 32(1)(a), considers it as one of the main security measures adopted by the controller and the processor in order to mitigate the risks for the data protection. So, the adoption of pseudonymization techniques allow the ANITA project to be compliant with the GDPR.

Table 26: Legal requirements – Data anonymization and pseudonymization

Requirement title (ID)	**Information to data subject in LEAs investigation activities** (LR_06)
Level of criticality	3
Definition and description	When processing personal data for the purposes of the Directive, in order to enable the data subject to challenge the legality of the processing of personal data concerning him/her, the data subject has the right to be informed as a principle, particularly where the data are collected without his/her knowledge. This principle is exempted when such information would jeopardize ongoing investigations, expose a person to a danger or harm the rights and freedoms of others. This right is particularly important for witnesses and non-suspects. So, when and if possible, the data subject will receive accurate and full information about the processing, including: (a) the identity and the contact details of the controller; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended; (d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority; (e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject. For example, LEAs will provide witnesses and non-suspects users with a privacy policy, specifying all the previous mentioned information about data collection and use.

Complementary explanations	Article 13 of the Directive sets out the minimum level of information to be given to any data subject. Article 13 also envisages the opportunity to share information about the legal basis for the processing, the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period, the categories of recipients of the personal data, including in third countries or international organisations and further information, in particular where the personal data are collected without the knowledge of the data subject. However, these kinds of information may be excluded from the information provided to the data subject if there is a Member state law that delays, restricts or imposes to omit them in order to avoid obstructing official or legal inquiries, investigations or procedures, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protect public security, protect national security or protect the rights and freedoms of others.

Table 27: Legal requirements – Information to data subject in LEAs investigation activities

Requirement title (ID)	**Distinction between different categories of data subject in LEAs investigation activities** (LR_07)
Level of criticality	3
Definition and description	Article 6 of the Directive distinguishes between different categories of data subjects: suspect, perpetrator, victims, witnesses, informants, contacts and accomplice. Such a distinction is also necessary to ensure proper implementation of the principles relating to data processing (e.g. transparency and information to be given to the data subject). The crucial importance of updating those data at the end of the investigation/judicial proceeding can also affect the Data accuracy and updating (LR_04) requirement.
Complementary explanations	The *Opinion 01/2013* of the Art. 29 WP insisted, in particular, on the category of persons which have no known relation to a crime, the so-called "non suspects". "*Processing of data of persons who are not suspected of having committed any crime (other than victims, witnesses, informants, contacts and associates) shall be strictly distinguished from data of persons related to a specific crime and "should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose." Furthermore, such processing should (in the view of the data protection authorities) "be restricted to a limited period and the further use of these data for other purposes should be prohibited." A specific protection of "non-suspects" is particularly required when the*

	processing is not done in a specific criminal investigation or prosecution". In other words, the distinction between different data subjects affects the application of many of the previous mentioned requirements such as: Lawfulness of the processing (LR_01), Purpose limitation (LR_02) Data minimization (LR_03) Data accuracy and updating (LR_04) Information to data subject in LEAs investigation activities (LR_06).

Table 28: Legal requirements – Distinction between different categories of data subject in LEAs investigation activities

Requirement title (ID)	**Security of personal data** (LR_08)
Level of criticality	3
Definition and description	• Personal data must be protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. Therefore, the storage will provide for data encryption and disassociation, protecting data against any illegitimate access by third parties, also ensuring data integrity against unauthorised modification. Each technical partner will responsible for hosting and managing its own components, providing all the information about security measures adopted to protect their databases. In order to ensure the security of the whole processing, the Consortium has appointed one of its Partners – the Italian Institute for Privacy (IIP) – which holds a sound and well-known expertise in data protection law, as its Data Protection Officer. It has also arranged physical, technical, and administrative measures to safeguard information in our possession against loss, theft and unauthorized use, disclosure, or modification (e.g. pseudonymization, expert processor, designed data protection officer etc.).
Complementary explanations	As a part of the security of the processing, the data controller/processor must take "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:* *(a) the pseudonymisation and encryption of personal data;* *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;* *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;* *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*" (Article 32(1) of the GDPR*)*. In the event that the data controller avail itself of a data processor, the

	latter must ensure security of processing (see Bind the processor to the controller requirement (LR_10). A similar provision is set out by Article 29 of the Directive with regard to: (a) deny unauthorised persons' access to processing equipment used for processing ('equipment access control'); (b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control'); (c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control'); (d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control'); (e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control'); (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control'); (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control'); (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control'); (i) ensure that installed systems may, in the case of interruption, be restored ('recovery'); (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity'). That is why the Consortium has set requirements for LEAs about: - Registration and authentication of LEAs officers (TR_SE_02) - Data integrity and confidentiality (TR_SE_03) and has applied to the final product offered to them the requirements of: - Data back-ups (GR_FR_02) - Role Based Access Control (GR_DBS _04) - Business Continuity (GR_DBS _05) - Reliability (TR_R_01) - Protection measures for interfaces (TR_SE_01)

	Moreover, according to ANITA project, as incorporated in the Grant Agreement signed with the EC (paragraph 5.1.5, page 262) "*ANITA will apply firewall and proxy technologies to protect the system from botnets and cyber-attacks. The policies to react to cyber-attacks will be set-up according to the risk assessment that will be performed before the deployment*".

Table 29: Legal requirements – Security of personal data

Requirement title (ID)	**Data breach communication** (LR_09)
Level of criticality	3
Definition and description	Users and Data Protection Authorities will be informed of any occurred breach of the security of the servers leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, as well as about any possible remedies.
Complementary explanations	During the Data Protection Office task, there will be implemented procedures for data breach communications both to authorities and data subjects according to: - Articles 33 and 34 for data breaches that can occurs during the research phase; - Articles 30 and 31 for data breaches occurred after the final product release to LEAs.

Table 30: Legal requirements – Data breach communication

Requirement title (ID)	**Binding the processor to the controller** (LR_10)
Level of criticality	3
Definition and description	Data processing by way of a processor must and will be governed by a writing contract or legal act, binding the processor to the controller (ANITA consortium) in order that the processor shall act only on instructions from the controller, respecting the same data storage security principles. A copy of this binding act will be available to the data subject upon request. Since the Consortium may engage technical partners as providers of technology, during the Data Protection Office task it will formally bound them by means of a data processing agreement, as per Article 28 of the GDPR. In any case, the full list of data processors is available by simple request to the data controller by sending an email to the Consortium.mailto:privacy@privacyflag.eu

Complementary explanations	In light of Article 28(4) of the GDPR, where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Table 31: Legal requirements – Binding the processor to the controller

Requirement title (ID)	**Prior notification replacement with data protection and ethics impact assessment** (LR_11)
Level of criticality	3
Definition and description	The obligation to notify the supervisory authority before carrying out any processing operation from Article 18 of Directive 95/46/EC was abandoned by the General Data Protection Regulation. From 25 May 2018, controllers (i.e. the Consortium) only need to consult the data protection authority in case that a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk (Article 36(1), GDPR). ANITA project will perform a data protection and ethical impact assessment in line with the GDPR before the tools development, in order to implement an ethics and data protection-by-design approach.
Complementary explanations	In light of Article 36(1), GDPR controllers are only obliged to assess the risks of their processing operations when the processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 35, 1 GDPR) or when the processing concerns a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing (including profiling), and on which decisions are based that produce legal effects or similarly significant effects to the natural person, when the processing concerns a large scale processing of special categories of data or of personal data relating to criminal convictions and offences, or when the processing concerns systematic monitoring of a publicly accessible area on a large scale (Article 35(2), GDPR), or when the competent data protection authority has listed the processing activity to be the subject of a data protection impact assessment (Article 35(4), GDPR). As some of these requirements may apply to ANITA's outputs (e.g. tools),

	the ANITA project will perform a data protection and ethical risk assessment in line with the GDPR before the tools development. ANITA aims to comply with the highest standards of protection of natural persons, hence, a data protection and ethics impact assessment is included in the work structure of the project under the supervision and guidance of the Data Protection Officer (T3.4).

Table 32: Legal requirements – Prior notification replacement with data protection and ethics assessment

Requirement title (ID)	**Appropriate retention period** (LR_12)
Level of criticality	3
Definition and description	During the project lifetime, only personal data of researchers, LEAs, testers or any involved person who provides his/her personal data will be kept until the end of the project itself. Any other personal data collected by error will be deleted (see Incidental personal data collection (GR_DM_01) requirement After the end of the project, in real operational scenario, the personal data will not be kept longer than necessary according to the national legislation of the LEA using the tool.
Complementary explanations	The developed system will use cryptographic and data isolation technologies and will ensure that all the evidence will be destroyed at the end of the pilots' execution for suspected traffickers personal data, or until they have been detected for incidentally collected personal data (no later than the end of the project). It is important to underline that after the final product release, the retention period for LEAs depends on Member States law according to Article 5 of the Directive which states that: "*Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed*".

Table 33: Legal requirements – Appropriate retention period

Requirement title (ID)	**Right of access** (LR_13)
Level of criticality	3
Definition and description	The Consortium, acting as the data controller, will avoid any personal data collection, adopting also Incidental personal data collection (GR_DM_01) procedure. Anyway, it must ensure that the right of access exercised by data subjects is enforced. Every data subject will have the right to obtain from the controller, without

	excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to the purposes of the processing, the categories of data concerned, and the recipients to whom the data are disclosed. This means that user's requests must be conveyed to a single point of contact able to promptly respond to them. The systems will be designed so as to make sure that all such similar requests are conveyed to a single point of contact managed by the Consortium Data Protection Office (IIP) which will assess them against the law, provide required feedback to the users and have them enforced, as the case may be, by the Consortium. For example, each cyberspace user can contact the data processor (the Consortium), via email (the address will be activated during T3.3) in order to assert the confirmation of the existence of data concerning him/herself and their origin/purposes thereof.
Complementary explanations	The legal source of this requirement is Article 15 of the GDPR. It is important to underline that after the final product release, the exercise of the right of access during LEAs activities depends on Member States law according to Articles 14-15 of the Directive which states that: "*Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society*".

Table 34: Legal requirements – Right of access

Requirement title (ID)	**Right of erasure** (LR_14)
Level of criticality	3
Definition and description	The Consortium, acting as the data controller, will avoid any personal data collection, adopting also Incidental personal data collection (GR_DM_01) procedure. Anyway, it must ensure that the right of erasure exercised by data subjects is enforced, when the conditions set out by law are met. The systems will be designed so as to make sure that all such similar requests are conveyed to a single point of contact managed by the Consortium Data Protection Office (IIP) which will assess them against the law, provide required feedback to the users and have them enforced, as the case may be, by the Consortium. For example, by contacting the data controller (the consortium) via email can ask the cancellation of his/her personal data, with the certification that the operation has been brought to the attention of those to whom the

	data were communicated or disseminated.
Complementary explanations	This obligation stems from Article 17 of the GDPR. Having regard to final product used by LEAs, it is paramount to underline that the right to erasure is linked to different factors: first of all, it has to be executed where processing infringes the principles of processing, the provisions about lawfulness of the processing and the special categories of personal data dispositions, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject. Secondly, instead of erasure, the controller shall restrict processing where: (a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or (b) the personal data must be maintained for the purposes of evidence. As for the right of access, the controller has to inform the data subject, in writing, of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. However, it is up to Member States to adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned (Article 16). It means that, as for the **Right of access** (LR_13), the right of erasure depends on the Member State law.

Table 35: Legal requirements – Right of erasure

Requirement title (ID)	**Universality of data protection standards** (LR_15)
Level of criticality	2
Definition and description	All the privacy and personal data protection standards are applied to all cyberspace users, regardless of their country of residence. In fact, each tool will have the same functionalities despite the users' homeland and each right will be guaranteed, applying the public international law, the European primary and secondary law (e.g. all the users can contact the data controller – the consortium - via email at …@...).
Complementary explanations	Privacy and personal data protection standards are guaranteed at many levels. First of all, at the level of Public International Law (*European Convention of Human Rights* (Article 8 – respect of private life); *Convention n. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Articles 5, 6, 8, 9 – data quality, special category of data, safeguards of the data subject, exceptions and restrictions).

	Secondly, at the level of European Primary Law (*Charter of the Fundamental Rights of the EU* (Articles 7 – private life –, 8 – personal data); *European Treaties (TEU* – Article 6, *TFEU* – Article 16). Lastly, at the level of European Secondary Law (*679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation; Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA)*. Therefore, the previously mentioned standards are applied to all users, regardless of their country of residence.

Table 36: Legal requirements – Universality of data protection standards

Requirement title (ID)	**Personal data transfer** (LR_16)
Level of criticality	2
Definition and description	ANITA ensures to avoid any personal data transfer to third parties, except in case of legitimate requests by a competent public authority or in case when transfer is mandated by law. For example, the Consortium may share personal data with any partner to the Consortium, as well as with its affiliates-companies that control, are controlled by, or are under common control with any of the Consortium's Members. These entities may receive this information only to the extent necessary for the proper execution of the research activities, or for the administration of the project. There may be also instances when the consortium discloses information to other parties in order to: • protect the legal rights of the Consortium, its partners and the latter's affiliates, and of the users of the Services; • protect the safety and security of cyberspace users (e.g. data breaches); • prevent fraud (or for risk management purposes); or • comply with or respond to the law or legal process or a request for cooperation by a government entity, whether or not legally required; • administer the project and share the results thereof with the European Commission or any other public authority to which the Consortium, or any of its Partners, has to report.

	In case of need, the information sharing with third parties will occur only in aggregated or non-personally identifiable form.
Complementary explanations	According to ANITA project, as incorporated in the Grant Agreement signed with the EC (paragraph 5.1.3, page 260), "*ANITA consortium contains a non-EU country – Serbia*". As also stated in the Grant Agreement, AoC is the leader of Task 11.4 – Training activities, and, based on the aims of this task, AoC will organise training activities of officers of different LEAs and other relevant stakeholders, in order to equip them with comprehensive knowledge and effective skills to recognize and address illegal trafficking activities and to facilitate cooperation among LEAs. Training activities will be realised in the form of workshops, webinars, professional courses and face-to-face meetings, at individual-level, institutional-level and societal-level. In order to achieve the above aims of the task, AoC will be requested to access the personal data of the officers who are employees of the organisations that are/will be part of the ANITA User Community, which is managed by DITSS (User Community Manager). Therefore, a transfer of personal data from EU (Netherlands) to a third country (Serbia) will take place. As, so far, there is no adequacy decision by the European Commission on Serbia, the Consortium will use European Commission standard data protection clauses which are a proof of adequate data protection standards. Due to the relationship between DITSS and AoC, we consider them both data controllers, therefore it will be used the controller-to-controller standard clauses (for further details see D12.3).

Table 37: Legal requirements – Personal data transfer

Requirement title (ID)	**Accountability** (LR_17)
Level of criticality	3
Definition and description	By producing all the relative documents (e.g. records of processing activities, processors designation, data breach procedures, ethics and privacy policy internal, confidential data protection policies, datasets sharing agreements etc.) the Controller (i.e. the consortium) will be responsible for and be able to demonstrate compliance with the GDPR and to have taken into account the potential issues of the final product when used by LEAs (Directive 680/2016).
Complementary explanations	During Task 3.3 – Data Control, will be drafted of all the compliance documents and internal procedures in order to be fully aligned with EU law and Ethics principles and coordinate Consortium's compliance actions as

	defined during T3.1 with the set of requirements. In order to adopt a data protection and ethics by design approach, during Task 3.4, on the basis of a comparative analysis of the social, ethical, legal, privacy requirements emerged in Task 3.1, the critical aspects will be defined during the tools development. In order to do so, all the possible impacts on the rights of individuals involved in the project activity (on line users, researchers, third parties) will be assessed, so as to identify related solutions/mitigation measures. The impact assessment will be carried out also for researchers involved in the project. In fact, there are possible ethical and legal risks for them, in light of the likely sensitiveness and side effects of the envisaged research activity in dark web. The task aims to do a legal and ethical assessment of the various components of the project (i.e. tools, systems) following the outputs of Tasks T3.1 and 3.2 and a) searching the impact of the technology; b) searching the extent in which fundamental social, ethical and legal goods (including privacy) may be infringed; c) searching the impact on the limitations of rights and freedom generated by the tools developed in the project. As output of the task, at the end of the assessment, an awareness report will be produced, in order to balance the underlined risks with mitigation measures applying an Ethics-by-Design and Data Protection-by-Design strategy.

Table 38: Legal requirements – Accountability

3.4.4 Ethical requirements (ER)

Requirement title (ID)	**Ethical-driven approach** (ER_01)
Level of criticality	3
Definition and description	The tools and the platform must be designed to address the ethical requirements and implement an ethical-by-design approach, including ethical guidelines for the usage of the final product by LEAs.
Complementary explanations	Ethical requirements will be built on the ethical principles constituted in the Charter of Fundamental Rights of the European Union (CFREU) and the European Convention on Human Rights (ECHR) and all other applicable international and EU legislations. Particularly, ANITA will aim to ensure respect for people and human dignity, fair distribution of research benefits and burden and protecting the values, rights and interests of the research participants. Even if ANITA does not involve single human being but focuses on the monitoring of illegal activities and of anonymous groups only, the research results have the potential to be misused because the technologies developed by the ANITA consortium could have a severe negative impact on human right

	standards if they are misapplied. In order to prevent any (intentional or unintentional) bias existing ex ante, prior to the design and development of the system, the designer's values or the values of end-users (LEAs) should be guided by common principles to be embedded into the system and reported in an ethical document (e.g. guidelines) to be followed by LEAs at the end of the products development.

Table 39: Legal requirements – Ethical-driven approach

Requirement title (ID)	**Human dignity and misuse prevention** (ER_02)
Level of criticality	3
Definition and description	Human dignity which includes respect for private and family life (Article 7, CFREU and 8, ECHR), protection of personal data (Article 8, CFREU), freedom of expression and information (Article 11, CFREU) which has to be interpreted as the right produce/publish/transmit/share data (active profile), but also to be able to be informed by those who prepare and transmit news of public interest (passive profile) and also to be able to access that news. Already if these three basic profiles are considered, it is clear that such freedom is also founded on the right to research information and sources and on guarantees of pluralism.
Complementary explanations	Human dignity is one of the main ethical principles to be taken into account, according to Article 1, CFREU. Particularly, ANITA will aim to ensure respect for Privacy and data protection but also right of expression, in order to avoid any limitation. For its very nature, the dark web allows freedom of information also in case of non-democratic environments (e.g. journalists activities). In order to prevent any potential misuse of the tools employed by the project made by undemocratic governments and in order to better understand how to cooperate against illegal trafficking crimes with law enforcement agencies without compromising the democratic European asset, ANITA will define the effective cooperation with LEAs involved in the project through cooperation agreements or "informal" trusted network.

Table 40: Legal requirements – Human dignity and misuse prevention

Requirement title (ID)	**Equality and non-discrimination** (ER_03)
Level of criticality	3

Definition and description	Equality and non-discrimination which includes equality before the law (Article 20, CFREU) and prohibition of any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation (Article 21, CFREU), which is linked to the freedom of thought, conscience and religion (Article 10, CFREU).
Complementary explanations	Even if ANITA research main purpose is to monitor anonymous groups only, there could be cases in which discrimination can be a risk – for example in monitoring extremist (religious) groups activities, to assess terrorism fundraising or conversation in a certain language/dialect linked to the known traffickers' ethnic origins. That is why ANITA will aim to ensure respect for freedom of thought, conscience and religion, in order to avoid any discrimination based on sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. Any automatic interdependencies and syllogism between certain human characteristics (e.g. being Muslim) and the belonging to terrorist or criminal group will be avoided.

Table 41: Ethical requirements – Equality and non-discrimination

Requirement title (ID)	**Automated individual decision-making, including profiling** (ER_04)
Level of criticality	3
Definition and description	Automated individual decision-making, including profiling, is regulated by the data protection legal background (Article 22, GDPR and Article 11, Directive). However, given to ANITA research purposes and final product capabilities, to be subject to a decision based solely on automated processing, including profiling, could produce legal effects concerning cyberspace users.
Complementary explanations	The research phase will not allow to take automated decision and profiling cyberspace users without the human intervention. This asset will lead to a final product in which the automated individual decision-making is not available for cyberspace users profiling but only for the automated processing of investigation data such as texts, images/videos, audios to handle with specific contents, languages, terminology, vocabulary, symbols, pictures, etc. related to the considered crimes and NOT to specific automated profiling activity.

Table 42: Ethical requirements – Automated individual decision-making, including profiling

Requirement title (ID)	**Presumption of innocence and legality of penalties** (ER_05)
Level of criticality	3
Definition and description	Presumption of innocence and right of defence guarantee that everyone who has been charged shall be presumed innocent until proved guilty according to law. Moreover, it is not possible to declare someone guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national law or international law at the time when it was committed.
Complementary explanations	Article 48, CFREU avoids any illicit interpretation of the charges, so until proved guilty by the judge, anyone has the right to be presumed innocent and to defend him/herself. Article 49, CFREU excludes the possibility to retrieve old gathered/stored data in order to charge someone of crimes which did not constitute a criminal offence under national law or international law at the time when it was committed.

Table 43: Ethical requirements – Presumption of innocence and legality of penalties

Requirement title (ID)	**Limit minors of age involvement** (ER_06)
Level of criticality	3
Definition and description	Since ANITA research will NOT include children involvement, if someone become aware that a minor has been involved in ANITA research or affected by ANITA monitoring tool, can contact the data controller (the Consortium) via email or, if the Consortium itself becomes aware that a child has been involved, it will take steps to remove promptly such information.
Complementary explanations	ANITA research will NOT include children (as stated in the G.A. paragraph, 5.1.1, page 258) and Incidental personal data collection (GR_DM_01) requirement will be applied to minors' personal data incidentally collected with undue delay.

Table 44: Ethical requirements – Limit minors of age involvement

3.4.5 Other requirements (OR)

Requirement title (ID)	**End-user driven approach** (OR_01)
Level of criticality	3
Definition and description	The tools and the platform must be designed to address the end-user needs and requirements pointed out in WP4.
Complementary explanations	A key factor of success is the adoption rate of the developed tools by real end-users. The tools will accordingly be designed and tested with the end-user to align as much as possible with the end-user needs and expectations.

Table 45: Other requirements – End-user driven approach

Requirement title (ID)	**Risk management and minimization** (OR_02)
Level of criticality	3
Definition and description	The Consortium must properly mitigate and eventually externalize the legal and economic risk related to the exploitation of the results.
Complementary explanations	This requirement implies properly analysing and designing policies and ethical guidelines. It also requires dissociating activities which carry a legal or economic risk from the core project.

Table 46: Other requirements – Risk management and minimization

4 Conclusions

This Deliverable has presented all the requirements needed in order to provide a common vision on the architecture development that will be the subject of WP4. The document will serve as an input for the components design and implementation, taking into account all the legal and ethical implication of the project both from the research perspective and the final product usage.

Our research has analysed international and European obligations related to privacy, integrating them with an ethics-driven approach. For this reason, we had proceeded not just by identifying the legal framework but also introducing “ethical concerns” from the human rights and freedoms perspective.

Contributions given by all partners have helped to strengthen the cooperation across the consortium, by matching legal knowledges with future technical expertise applied to the tools implementation.

The set of systems requirements had been developed starting from all of this resources, providing not just a set of generic guidelines for the architecture development, but also a concrete basis to understand possible interactions between the system, the end-users and the cyberspace users.

During the lifecycle of the project, legal end ethical requirements will be surely further updated and monitored according to the feedback originating from the other Work Packages, and thanks to the continued cooperation between partners with different competencies. In fact, the project is entering in its operative phase, during which all the requirements will be tested, revised and modified according to the emerging needs.

5 References

Robertson, S. (2001). Requirements Trawling: Techniques for Discovering Requirements. *International Journal of Human-Computer Studies,* 55, pp.405-421.

Article 29 Data Protection Working Party, *Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, in* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf

Article 29 Data Protection Working Party, *Opinion 5/2014 on anonymization techniques,* Adopted on 10 April 2014, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, Adopted on 27 February 2014, in http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf

Article 29 Data Protection Working Party, *Opinion 03/2014 on Personal Data Breach Notification,* Adopted on 25 March 2014, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation,* Adopted on 2 April 2013, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices,* Adopted on 27 February 2013, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party, *Opinion 04/2012 on Cookie Consent Exemption,* Adopted on 7 June 2012, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent,* Adopted on 13 July 2011, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party, *Opinion 14/2011* and Annex *on data protection issues related to the prevention of money laundering and terrorist financing, in* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data,* Adopted on 20 June 2007, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International*

Data Transfers, Adopted on 3 June 2003, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Charter of Fundamental Rights of the European Union, 2012/C 326/02, in eur-lex.europa.eu

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, in www.coe.int

Convention on the Rights of Persons with Disabilities, New York, 13 December 2006, in www.ohchr.org

Convention on the Rights of the Child, New York, 20 November 1989, in www.ohchr.org

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, in eur-lex.europa.eu

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 *amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, 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*, in eur-lex.europa.eu

Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 *concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, in eur-lex.europa.eu

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*, in eur-lex.europa.eu

European Convention on Human Rights, Council of Europe, Rome, 4.XI.1950, in http://www.echr.coe.int/Documents/Convention_ENG.pdf

International Covenant on Civil and Political Rights, New York, 16 December 1966, in www.un.org

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, New York, 18 December 1990, in www.ohchr.org

ITU report on Quality of Services for Wireless Fixed Communication Systems), in http://www.itu.int/pub/r-rep

Regulation 679/2016, adopted on 4 May 2016, in http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1465303957140&from=EN

Regulation 45/2001/EC of the European Parliament and of the Council *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*, in eur-lex.europa.eu

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, in eur-lex.europa.eu