PUBLIC

CounteR

Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection

Project Acronym	CounteR
Project Full Title	Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection
Grant Agreement no	101021607
Project Duration	36 months (starting May 1st 2021)

Deliverable number 1.3

Review of relevant supranational/EU/national laws and regulations

Work Package	WP 1 – System Specification & Architecture
Task	Task 1.3 – Definition of the legal requirements of the solution
Lead Beneficiary	MITLA
Due Date	30/11/2021
Submission Date	30/11/2021
Deliverable Status	Final version
Deliverable Type	R (Report)
Dissemination Level	PU
Document Name	D1.3 – Review of relevant supranational/EU/national laws and regulations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

PUBLIC

Editors

Surname	First Name	Beneficiary
Zammit Maempel	Michael	MITLA

Contributors

Surname	First Name	Beneficiary
Cannataci	Sarah	MITLA
Trufin	Catalin	AST
Luzon Tuells	Joaquín	INS
Tantu	Dana	INS
Kostadinov	Georgi	IMG
Castillo	Ian	ICON
Malerba	Donato	CINI
Seddah	Djamé	INRIA
Pollner	Peter	ELTE
Barbara	Lucini	UCSC
Mavrov	Borislav	EI
Nagem	Rasha	MDS
Zamorano	Mariano Martín	ETI
Theodoropoulos	Konstantinos	FNET (NOVA)
Farinha	Cristina	PJ
Stangl	Stephanie	HFoD
Einats	Kaspars	SPLV
Roman	Razvan	SPP
Lasov	Yordan	BGP

Reviewers

Surname	First Name	Beneficiary
Zammit Maempel	Michael	MITLA

History of Changes

Version	Date	Change	Modified by
0.1	15.09.2021	Proposed Outline	Sarah Cannataci (MITLA)
0.2	22.09.2021	Content	Sarah Cannataci (MITLA)
0.3	25.10.2021	Quality check	Michael Zammit Maempel (MITLA)
0.4	Various	Addition of specific content	Members of Consortium
1.0	29.11.2021	Final review	Sarah Cannataci (MITLA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

Executive Summary

This deliverable forms part of Work Package 1 (WP1), titled 'Systems Specification & Architecture'. The aim of the entire WP1 is that of defining the specification requirements for each of the use cases and more importantly, the design of the overall architecture of the CounteR solution ('the Solution').

The CounteR Project (the 'Project') will combine state of the art NLP technologies with expert knowledge into the psychology of radicalisation processes, with the aim of creating the Solution which will allow early alert, analysis and prediction platform for data mining. The Solution will incorporate a variety of information sources, being both online and offline in nature, which in turn, will allow law enforcement agencies ('LEAs') to share information and take coordinated action in real time to help combat propaganda, fundraising, recruitment and mobilization, networking, information sharing, planning/coordination, data manipulation and misinformation related to radicalisation.

The aim of this deliverable is to specify the legal principles and requirements that the Solution must satisfy throughout development, as well as piloting and implementation stages which will involve processing of personal data by LEAs. Given that this deliverable is being drawn up at the initial stage of the project at a time when the requirements of the data processing, fusion and interpretation methods of the Solution are still in the process of being identified, this deliverable proposes a pre-emptive legal framework for the Solution, and in turn, the Project, to be guided by.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

List of Abbreviations

Term	Definition/Description
DPA	Data Protection Authority or Supervisory Authority
EU	European Union
GDPR	General Data Protection Regulation or Regulation [EU]2016/679
LEA	Law Enforcement Agency

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

1 Introduction

1.1 Relation with other tasks and deliverables

This deliverable is related to the following other Project tasks and deliverables:

Table 1 - Relation to other deliverables

Deliv.#	Deliverable Title	Nature of Relation
D1.2	Technical Requirements	D1.2 establishes the requirements for the development of the Project, particularly the technical components of the same, the integration of which is considered in D1.3, whilst the latter also sets out the requirements which will guide the data processing considered in D1.2. The two deliverables therefore both receive and provide input to each other and are inter-linked.
D7.1	Data Protection requirements	D7.1 establishes the data protection requirements of the Solution, and this by framing the legal requirements and principles that are explored within D1.3.
All tasks	Covers a variety, if not all, of the tasks and deliverables forming part of this Project	D1.3 sets out the legal requirements which will guide the Project throughout development and pilot stage.

1.2 Methodology

The DoA describes this deliverable as:

- *D1.3: Review of relevant supranational/EU/national laws and regulations*
- *Report on legal requirements of the solution in regards to privacy and personal data protection, including all levels of laws and regulations (supranational, EU, national-level laws of all EU member states).*

The main objective of this document is to broadly identify the legal requirements for the development of the Solution relating to privacy and processing of personal data across the European Union, for the deployment of the Solution in the piloting and implementation stages within the jurisdictions from which the six (6) LEAs originate, that is (i) Portugal; (ii) Latvia; (iii) Romania; (iv) Bulgaria; (v) Germany and (vi) France. Therefore, while D7.1 focuses on requirements for the solution deployment, addressing aspects such as ethics and privacy by design, D1.3 provides requirements to ensure that all piloting and research activities conducted within CounteR comply with the EU legal framework.

To this effect, this Report sets out the legal principles guiding the development and piloting of the Solution in a two-fold manner; firstly, the Report sets out the main legal principles which apply to the development of the Solution, the majority of which arise almost exclusively from Regulation

[EU] 2016/679[1]; and secondly, the Report sets out the legal principles which are applicable at the stage of piloting and implementation by LEAs, which are regulated by supranational and national legislation regulating the same. In relation to the latter, since the LEAs originate from an EU Member State, they would be subject to, amongst others, a national transposition of Directive 2016/680[2].

The first part of the Report was undertaken through a comparative review of freely accessible documentation by the legal experts of MITLA, whilst the second part of the Report was supplemented with information provided by the LEAs and the members of the Consortium on national requirements to which they are subject. This approach then allowed the relevant legal principles and requirements applicable to the Solution to be set out within the Report in a more easily accessible format.

1.3 Deliverable structure

This document includes the following main sections:

- **Analysis of EU & International laws relating to development of Solution** – describing a thorough analysis of all EU and International laws that relate to the development of the CounteR solution.
- **Analysis of EU, International and national laws relating to processing of personal data by LEAs** – offering a comprehensive picture of the EU, international and national laws that focus on the processing of personal data by LEAs.
- **Legal Principles** – section that includes the legal principles and requirements sustaining the development and piloting of the CounteR solution to support the members of the Consortium, mainly technical partners and LEAs.
- **Conclusion** – providing final conclusions related to this deliverable.

[1] *Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*

[2] *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*

2 Analysis of EU, International and national laws relating to the development of the Solution

The objectives of the Project can be achieved by the Solution only through the processing of personal data. As a result, the processing of personal data is a central feature of the Solution and therefore the Solution must be developed in a manner that is compliant with data protection law, and which allows the continued compliance with obligations arising from the laws on privacy. This section will assess the current applicable laws relating to the processing of personal data as relevant to the development of the Solution during the course of the Project.

2.1 EU Standard - Regulation 2016/679

Regulation 2016/679, or as it is more commonly referred to, the General Data Protection Regulation (the 'GDPR'), is the principal legislation forming part of the current data protection framework within the EU. Since coming into force on the 25th May 2018, the GDPR has harmonized the approach to data protection in all twenty seven (27) EU Member States. The latter has been achieved due to the nature of the GDPR as a legal instrument – being a regulation, the GDPR must be applied in its entirety across the EU[3] in the same way. Since the entirety of the Consortium is based within the EU, the development stage of the Project is subject to the GDPR as the main applicable piece of legislation on data processing, along with any other supplementary national law on data protection. In light of this, an analysis and proper understanding of the GDPR is crucial to allow the identification of the legal principles underpinning the Project.

2.1.1 Scope

The scope of the GDPR is two-fold in nature; (i) material; and (ii) territorial. From a material point of view, the GDPR does not apply all processing operations of personal data. Particularly relevant to the Project, it must be noted that activities which fall outside the scope of EU law (such as activities concerning national security), and 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, including the safeguarding against and the prevention of threats to public security, are not subject to the GDPR.

From a territorial aspect, the GDPR applies to the processing of personal data undertaken by data controllers or processors which are established within the EU, regardless of whether the actual processing of personal data takes place within the EU. In addition, the GDPR applies to the processing of personal data by entities which are not established within the EU, where:

a) The entities are located within a jurisdiction that EU Member State law applies by virtue of public international law;
b) The processing relates to the offering of goods or services to individuals (data subjects) who are within the EU; or

[3] *Regulations, Directives and other acts | European Union (europa.eu)*

c) The processing relates to the monitoring of the behaviour of data subjects, where that behaviour takes place within the EU.

As a starting point therefore, it is evident that the processing of personal data during the development of the Solution by members of the Consortium (other than LEAs) satisfies both the territorial and material scopes of the GDPR and is thus subject to the same.

2.1.2 Interpretation

In order to undertake an in-depth study of the rules which regulate the development of the Solution, it is crucial to frame the discussion with the relevant definitions of terms and concepts which are central to the GDPR. Terms[4] pertinent to the current analysis are set out below:

i. **Data Subject** is defined as an identified or identifiable living natural person;
ii. **Personal data** is defined as any information relating to a data subject;
iii. **Processing** is defined as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
iv. **Profiling** is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
v. **Pseudonymisation** is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
vi. **Controller** is defined as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
vii. **Processor** is defined as natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

2.1.3 Data Protection Principles

The core data protection principles as originally set out within the GDPR's predecessor, Directive 5/46/EU, have been re-affirmed and further developed within the GDPR. Effectively, the obligations and rights recognized by the GDPR are all derivates of these principles, and in fact, the majority of the fines handed out across the EU since the coming into force of the GDPR relate to breach of one (or more) of the core principles of data protection. The processing of personal data subject to the GDPR must therefore be made in compliance with the following cumulative principles:

[4] *As defined within Article 4 of Regulation 2016/679.*

i. **Principle of lawfulness, fairness and transparency**
The processing of personal data must be made lawfully, fairly and in a transparent manner in relation to the data subject.

ii. **Principle of purpose limitation**
The processing of personal data must be made for specified, explicit and legitimate purposes and the personal data must not be further processed in a manner that is incompatible with those purposes.

iii. **Principle of data minimization**
The processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the personal data was originally processed.

iv. **Principle of data accuracy**
The personal data processed must be accurate and, where necessary, kept up to date.

v. **Principle of storage limitation**
The personal data must not be processed for a period longer than is necessary for the purposes for which personal was originally processed.

vi. **Principle of integrity and confidentiality**
The processing of personal data must ensure appropriate security of the personal data.

vii. **Principle of accountability**
The controller undertaking the processing shall be responsible for, and be able to demonstrate compliance with the data protection principles as listed above (i-vi).

Where, in the course of the development of the Solution, personal data will be processed, it must be ensured that the aforementioned principles are complied with and practiced. More detailed requirements as linked to these core principles are included within Section 4: Legal Principles below. In this regard, the Project must be guided by the concept of 'privacy by design', that is, at the moment when the technology underpinning the Solution is designed and created, data protection is integrated therein.

2.1.4 Legal basis

As a rule, and as tied to the principle of lawfulness, fairness and transparency, a valid lawful basis must serve as the foundation for any processing operation. The appropriateness of the legal basis underlying a processing operation depends on the purpose for the processing as well as the relationship that the data controller has with the data subject. The lawful basis must be determined and documented prior to initiating processing, and unless justified, the lawful basis should not be 'swapped' for another different lawful basis at a later date. It must also be noted that where the processing operation involves the processing of data which falls within the definition of special categories of personal data[5], a lawful basis must be identified not only for the general processing, but additionally, a lawful basis for the special processing must be identified.

At least one of the following legal bases must apply when personal data is being processed:

[5] *Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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.*

i. **Consent** – the data subject has given his clear and unambiguous consent to the processing of their personal data for a specific purpose;
ii. **Contract** – the processing is necessary for a contract that the controller has with the data subject, or because the data subject has request the controller to take specific steps ahead of entering into the contract;
iii. **Legal Obligation –** the processing is necessary for the controller to comply with legal obligations set out in EU or Member State law;
iv. **Vital Interests -** the processing is necessary to protect the data subject's life;
v. **Public Interest** - the processing is necessary for the controller to perform a task in the public interest or to fulfill the controller's official functions, which interest or function is set out in EU or Member State law;
vi. **Legitimate Interest** – the processing is necessary for the legitimate interests being pursued by the controller or a third party, unless the interests are overridden by the interests or rights of the data subject.

In this discussion, it is crucial to understand the concept of 'necessity' vis-à-vis a legal basis. A lawful basis will not be applicable if the purpose for the processing can be reasonably achieved by processing less data; or by implementing less intrusive means.

As aforementioned, the Solution will work using information arising from different sources. At the stage of development of the Solution, the members of the Consortium that will be processing personal data alone or jointly with others, must determine the relevant basis for the processing operation prior to initiating the same. Once identified, the legal basis must be recorded accordingly.

2.1.5 Data Subject Rights

Coming into force over 20 years after its predecessor, the GDPR built on the concerns and topical issues raised since the coming into force of Directive 95/46/EC by being a lot more data subject-centric. To this effect, the GDPR established a large variety of rights available to the data subject vis-à-vis data protection. Data subject rights are not absolute. In fact, the GDPR acknowledges that certain rights can only be exercised in particular conditions, whilst others are subject to a variety of exceptions. A total of eight (8) rights are available to data subjects, as set out below:

i. **The right to be informed**

The data subject has the right to be aware of the processing of their personal data - controllers need to be clear with about how they process data subjects' personal data. This right is linked to the principles of lawfulness, fairness and transparency. The clear and concise information must be provided to the data subject at the time it is collected from them, or where it is obtained from other sources, it must be provided within a reasonable period from obtaining the data, but no later than one month.

ii. **The right of access**

The data subject can access the personal data the controller holds about them and receive a copy of the personal data, along with other supplementary information. The information must be disclosed securely, and a controller may ask to receive proof of identity in order to ensure that the personal data is being released to the right person.

iii. **The right to rectification**

The data subject has the right to request the correction of inaccurate personal information the controller holds. This right allows the controller to continue to comply with the principle of data accuracy.

iv. **The right to erasure**
The data subject has the right to request the deletion of their personal data. In spite of a request for erasure, the controller may be justified to keep personal data which it needs to keep and this in accordance with exceptions set out within the GDPR.

v. **The right to restrict processing**
The data subject has the right to request the restriction or suppression of their personal data. In this regard, the controller is still permitted to store the personal data, but will not be able to process it otherwise.

vi. **The right to data portability**
The data subject has the right to request that the controller transfers or ports elements of their data to another service provider. A copy of the personal data is provided in a structured, commonly used and machine-readable form, however the controller is not required to adopt processing systems that are compatible with another organization.

vii. **The right to object**
The data subject has the right to stop the processing of their personal data for direct marketing, and also have the right to object to the processing in other particular situations. The controller will be able to continue processing the personal data if it can show that it has a compelling reason to do so.

viii. **Rights related to automated decision making including profiling**
The data subject has the right to request human intervention if automated processing without human intervention is used to make decisions having legal or similar effects on the data subject. This right is subject to specific exceptions, such as where the automated processing, including profiling, is authorized by EU or Member State law to which the controller is subject.

The GDPR also set out that where the processing is based on consent, the data subject shall have the right to withdraw consent for other consent-based processing at any time. In addition, the GDPR also sets out that data subjects have the right to lodge a complaint with their relevant supervisory authority.

Where personal data is to be processed in the development of the Solution, the members of the Consortium must ensure that they do not only implement measures to allow the exercise of rights by data subjects, but also that, where applicable, the rights of the data subjects are fulfilled within one (1) month, or where the particular request is complex, within a further two (2) months.

2.1.6 Data Transfers

The GDPR has strengthened the data protection framework across the EU Member States and further enunciated its territoriality aspect, and this by stipulating that any transfers of personal data to countries outside the EU (referred to as 'third countries') or other international organization shall be subject to strict rules. In this regard, the members of the Consortium involved in the development of the Solution must keep in mind that should the transfer of personal data to third countries or

international organizations be required, that transfer can only be undertaken subject to adequate data transfer tools as set out in the GDPR.

2.2 International Standards

The right to privacy and the protection of the same is enshrined internationally through a variety of different legislative instruments. The majority of these legislative instruments pre-date the GDPR by numerous decades, and therefore cannot be compared to the robust and specific of the GDPR as explored above. Nevertheless, the obligations set out within these international documents are as onerous as those set out in the GDPR, and therefore the legal principles arising from the same form part of the legal framework applicable to the development of the Solution.

Of particular relevance in this discussion are the following international standards:

- **Article 12, Universal Declaration on Human Rights**

  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.[6]

- **Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms**
  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 well-being 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.*[7]

2.3 National Standards

As noted above, the GDPR eradicated the fragmented approach to data protection that existed within the EU in the past. The GDPR did however leave some minor points on the regulation of data protection at the discretion of the EU Member States. In this regard, in order to cater for the members of the Consortium that are to be involved in the development of the solution, information on the legal framework vis-à-vis protection of personal data was requested from the Members of the Consortium who are envisaged to be involved in processing operations, which information is being replicated here:

Table 2: Information on legal framework within relevant jurisdiction by Consortium Member

Partner: AST | Jurisdiction: Romania

[6] *Article 12, Universal Declaration of Human Rights, United Nations General Assembly Resolution 217A*
[7] *Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms*

Legal Framework:

- GDPR
- ISO 27001
- Law no. 102 of 3 May 2005 on the establishment, organization and functioning of the National Authority for the Supervision of Personal Data Processing, with subsequent amendments and completions - Republic
- Law no. 129 of 15 June 2018 for the amendment and completion of Law no. 102/2005 regarding the establishment, organization and functioning of the National Authority for the Supervision of Personal Data Processing, as well as for the abrogation of Law no. 677/2001 for the protection of individuals regarding the processing of personal data and the free movement of such data
- Law no. 190 of 18 July 2018 on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals regarding the processing of personal data and on the free movement of such data; and repealing Directive 95/46 / EC (General Data Protection Regulation)
- Regulation of Organization and Functioning of ANSPDCP of 11 November 2005, with subsequent amendments and completions
- Law no. 682 of 28 November 2001 on the ratification of the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data, adopted at Strasbourg on 28 January 1981
- Law no. 506 of 17 November 2004 on the processing of personal data and the protection of privacy in the electronic communications sector
- Methodological norms of 20 November 2002 for the application of Law no. 365/2002 on electronic commerce
- Law no. 146 of 10 July 2008 for the accession of Romania to the Treaty between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on deepening cross-border cooperation and illegal migration, signed in Prum on 27 May 2005
- Law no. 363 of 28 December 2018 on the protection of individuals regarding the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating, prosecuting, and combating crime or the execution of punishments, educational and security measures, and on the free movement of these data
- Law no. 365/2002 on electronic commerce

Authorizations/Notifications Required: None

Other: None

Partner: INS | Jurisdiction: Spain

Legal Framework:

- GDPR
- Code regarding the protection of personal data (Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018), Measures, guidelines and directives,

ratione materiae, of the European Data Protection Board and of the National Supervisory Authority

- LOPDGDD – Organic Law 3/2018, Dec. 5th, Protection of Personal Data and Guarantee of Digital Rights (Ley Orgánica 3/2018, 5 de diciembre, de Protección de Datos Personals y garantía de los derechos digitales).

Authorizations/Notifications Required:

- INS is in the process of obtaining the acreditation ISO/IEC 27001, which is an international standard on how to manage information security.

Other: N/A

Partner: IMG | Jurisdiction: Bulgaria

Legal Framework:

- GDPR;
- Code regarding the protection of personal data (PERSONAL DATA PROTECTION ACT, amended SG No 93 of 26 November 2019), Measures, guidelines and directives, ratione materiae, of the European Data Protection Board

Authorizations/Notifications Required: None

Other: None

Partner: ICON | Jurisdiction: Malta

Legal Framework:

- GDPR
- Data Protection Act, Chapter 586 of the Laws of Malta
- Processing of Child's Personal Data in relation to the offer of Information Society Services Regulations, Subsidiary Legislation 586.11, which sets out that the processing of personal data of a child in relation to information society services shall be lawful where the child is thirteen years of age, in the absence of consent by the holder of parental responsibility over the child.
- Restriction of the Data Protection (Obligations and Rights) Regulations), Subsidiary Legislation 586.09, sets out the restrictions to the rights of the data subject as referred to in Article 23 of the GDPR, which restrictions in Maltese law are applicable where there are a necessary measure required for the safeguarding and maintain of national security, public security, defence and the international relations of Malta, as well as for the prevention, detection, investigation and prosecution of criminal offences, including measures to combat any money laundering activity, and the execution of criminal penalties, among other recognised circumstances.

Authorizations/Notifications Required: Chapter 586 sets out that a controller must consult with, and obtain prior authorisation from, the Data Protection Authority where the controller intends to process in the public interest: (a) genetic data, biometric data or data concerning health for statistical or research purposes; or (b) special categories of data in relation to the management of social care services and systems, including for the purposes of quality control, management

information and the general national supervision and monitoring of such services and systems. The law also sets out that where genetic data, biometric data or data concerning health are required to be processed for research purposes, the Data Protection Authority shall consult a research ethics committee or of an institution recognised by the Data Protection Authority.

Other: None.

Partner: CINI | Jurisdiction: Italy

Legal Framework:

- GDPR;
- Code regarding the protection of personal data (Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018), Measures, guidelines and directives, ratione materiae, of the European Data Protection Board and of the National Supervisory Authority;
- ISO/IEC 27001, ISO/IEC 27002

Authorizations/Notifications Required: None

Other: None

Partner: INRIA | Jurisdiction: France

Legal Framework:

- GDPR, (Legislative decree N°196/2003, as amended by Legislative Decree n°191/2018);
- "Loi Informatique et Liberté Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés" (Informatics and Freedom Bill, N°78-17 6/1/1978) amended by the legislative decree of 2019, June 1st.

Authorizations/Notifications Required: None

Other: None

Partner: ELTE | Jurisdiction: Hungary

Legal Framework:

- Article 12 (1) of the GDPR;
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information of Hungary;
- Data should only be processed for legitimate and duly specified (specific) purposes and only data strictly necessary for the fulfilment of those purposes.

Authorizations/Notifications Required: Data obtained from open sources: no prior authorisation/notification is required especially if the collected data is used for scientific purposes.

Classified information: based on the Act CLV of 2009 on the protection of classified information persons with special clearance can have access to classified information and sharing this information is restricted.

Other: ELTE has its own internal data management regulation. All researchers are requested to follow the guidelines described in it. The internal regulation is based on the EU GDPR regulations and the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information of Hungary. ELTE requires the development of a Data Management Plan for all projects.

Partner: UCSC | Jurisdiction: Italy

Legal Framework:

- GDPR;
- Code regarding the protection of personal data (Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018), Measures, guidelines and directives, ratione materiae, of the European Data Protection Board and of the National Supervisory Authority;
- ISO/IEC 27001, ISO/IEC 27002

Authorizations/Notifications Required: None

Other: None

Partner: EI | Jurisdiction: Bulgaria

Legal Framework:

- Personal Data Protection Act; In force as from 1 January 2002(amended SG No 93 of 26 November 2019) https://www.cpdp.bg/en/index.php?p=element&aid=1194

Authorizations/Notifications Required: None

Other: None

Partner: MDS | Jurisdiction: France

Legal Framework:

- According to Directive 2013/37/EU, known as PSI (Public Sector Information), and Law n°78-753 of July 17, 1978 (amended), known as CADA (Commission d'Accès aux Documents Administratifs), data resulting from a research activity financed at least for half by grants from a Public Institution, the State, local authorities, subsidies from national funding agencies or the European Union are considered as "administrative documents".
- As soon as they are considered as completed (notably after a first voluntary publication, such as a scientific publication) and if they do not fall within the legal exceptions (see particular cases below), they must be:
  - communicable to any person who requests it,
  - freely reusable.
- The Law n° 2016-1321 of October 7, 2016 for a Digital Republic goes further and modifies the code of relations between the public and the administration to move towards a principle of openness and spontaneous dissemination of data on the internet (open data), and free reuse without condition and for all purposes (including commercial purposes and including for public institutions). It neutralizes the right of databases for administrations, in its article 11.

- The Valter law specifies the principle of free access: re-use is free of charge, not subject to payment of fees. The re-use of public information is subject to the condition that the latter are not altered, that their meaning is not distorted and that their sources (authors and date of last update) are mentioned

Authorizations/Notifications Required: Special cases/Points of caution:

- Publication of personal data under conditions:
  - Personal (any information directly or indirectly identifying individuals or sets of data that, when cross-referenced, may identify individuals). The express agreement of the persons before the collection, the anonymization of the data before publication or at the end of the project and the access of the persons to their data during the project are compulsory (cf. RGPD, succeeding in 2016 to the Data-processing Law and Freedom)
- Data-processing Law and Freedom:
  - Law no. 78-17 of January 6, 1978 on information technology, files and freedoms :
  - Law no. 78-17 of January 6, 1978, relating to information technology, files and freedoms, better known as the loi informatique et libertés1, is a French law that regulates the freedom to process personal data2 , i.e. the freedom to file human beings. As this freedom is inseparable from computer activity, this law regulates the potentially anti-social consequences of computer activity.
  - Content of the law: Divided into thirteen parts, of which only the first three (Principles and definitions, Conditions of lawfulness of personal data processing, The National Commission on Data Processing and Liberties) directly concern individuals, the LIL places the legislation on data processing within the framework of human rights, certainly in memory of the purposes for which files were used under the Vichy regime.

Other: Prohibition of publication for data :

- relating to public security or defence secrecy (including those affecting the security of the institution's property or persons)
- relating to professional secrets (including process secrecy, medical secrecy, investigative secrecy, banking secrecy, business secrecy, including contracts and markets...)
- sensitive personal data: relating to racial or ethnic origins, political, philosophical or religious opinions, trade union membership, health or sex life, as well as biometric and genetic personal data allowing the unique identification of a physical person, passwords, banking or financial information, etc.

The collection and processing of such data is prohibited unless justified (in the public interest, for medical research...).

The authorization of the CNIL must be requested via the Data Protector Officer (DPO) or Data Protection Officer (DPD) of the organization.

Partner: ETI| Jurisdiction: Spain

Legal Framework: N/A

Authorizations/Notifications Required: N/A Other: N/A
Partner: Forthnet (NOVA) | Jurisdiction: Greece Legal Framework: ➢ In accordance with the GDPR and the Greek Legislation. The Company continuously assesses all new elements arising from the secure management of personal data and, if necessary, improves the relevant policies and practices it implements, in order to promptly respond to any eventual future changes. Authorizations/Notifications Required: None Other: None

3 Analysis of EU, international & national laws relating to the processing of personal data by LEAs

In order to obtain the objectives of the Project, once deployed, the Solution will involve the processing of personal data by LEAs. This section will assess the current applicable laws relating to the processing of personal data as relevant to the Solution, with a special focus on how the processing by the LEAs forming part of the Consortium is governed.

It has long been recognized that the processing of personal data by LEAs must be appropriately regulated and this to properly safeguard the fundamental rights and freedoms of individuals. The inherent nature of LEAs highlights a degree of imbalance of 'power' between the LEAs and the ordinary citizen. As a result, the processing of personal data by LEAs must be, and in fact has been, regulated separately to the processing of personal data by other types of persons.

3.1 EU & National Standards – Directive 2016/680

As noted above, 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, including the safeguarding against and the prevention of threats to public security, is excluded from the material scope of the GDPR. This subject matter however falls squarely within the scope of Directive 2016/680. The latter replaced Council Framework Decision 2008/977/JHA[8], and was adopted with the aim of allowing free flow of data between LEAs whilst ensuring the highest level of protection of personal data in these processing operations.

Directive 2016/680 does not have the same binding effect as the GDPR as a regulation. Whilst it is still a legislative instrument, a directive sets out a 'goal' that must be achieved by the EU Member States, leaving the actual transposition in the hands of the EU Member State. As a result, Directive 2016/680 set the benchmark for the EU legal framework in respect of processing of personal data by LEAs, both domestically and cross-border, as well as the exchange of information between police and judicial authorities. EU Member States were obliged to transpose the Directive 2016/680 by 6th May 2018.

As a result, outside of the processing of personal data in the development of the Solution, where personal data is processed by the LEAs in the piloting of the Solution, Directive 2016/680 will apply. The Directive excludes from its scope the processing of personal data; (i) in the course of an activity which falls outside the scope of EU law; and (ii) by EU institutions, bodies, offices and agencies. In regard to the exclusion noted in (i), it must be noted that 'activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU)'[9] falls outside the scope of EU law.

---

[8] *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.*

[9] *Recital 14, Directive 2016/680*

As a result, it may be difficult to assess the applicable guiding legislation in cases where the national law of the LEAs does not differentiate between national security and policing function. In order to cater for the LEAs which already form part of the Consortium of the Project, information on the legal framework vis-à-vis the transposition of the Directive 2016/680 was requested from the LEAs, which information is being replicated herein:

Table 3: Information on transposition of Directive 2016/680 within LEA jurisdiction

Partner: PJ | Jurisdiction: Portugal

Legal Framework:

- Law no. 59/2019, of 8 August - Approves the rules on the processing of personal data for the purposes of prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016
  - Article 1 - Object

    "This law establishes the rules on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, transposing into national law Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016."

  - Article 2 - Scope of application

    "1 - This law shall apply to the processing of personal data for the purposes referred to in the preceding article, in accordance with the criminal procedural law and other applicable legislation.

    2 - This law shall apply to the processing of personal data by wholly or partly automated means, as well as to the processing of personal data contained in a file or intended for such a file by non-automated means.

    3 - The present law shall not apply to the processing of personal data related to national security.

    4 - The exchange of personal data between competent authorities within the European Union, where legally required, shall not be restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

  - Assumptions underlying the data processing

    Its scope is the police functions of prevention and criminal investigation, prevention and repression of crimes. Intelligence services relating to national security are not included.

    The analysis of this project shall take into account the general principles and rules provided for by the GDPR, while the specific police, prevention and criminal investigation issues are regulated by Law 59/2019 of 08 August.

Authorizations/Notifications Required: N/A

Other: N/A

Partner: HfoD | Jurisdiction: Germany

Legal Framework:

- Federal Data Protection Act – new (BDSG – neu)
- Law on the Tasks and Powers of the Bavarian Police Force – (Polizeiaufgabengesetz - PAG)
- Code of Criminal Procedure (Strafprozessordnung – StPO)

Authorizations/Notifications Required: None

Other: None

Partner: SPLV | Jurisdiction: Latvia

Legal Framework:

Latvian State Police does social network content monitoring only within framework its competency. At the moment, it is possible to monitor the social networks at the organizational level (e.g., to prevent, investigate, detect criminal offenses), taking into account the requirements of the GDPR, as set out in Recital 19 of the same.

Doing monitoring o social networks is taking into account as well as Latvian legislation (e.g.: Personal Data Processing Law[10]). If necessary, during social network monitoring, personal data is not processed, but publicly available information is analyzed without identifying the persons who have posted the specific information on social networks (information source).

On the other hand, in cases where monitoring identifies a set of data that indicates a possible criminal offense (e.g.: threat of murder and serious injuries; incitement to terrorism and threat of terrorism; incitement to national, ethnic and racial hatred) in accordance with LV regulations, decisions will be made regarding the initiation of specific proceeding (e.g.: initiation of criminal proceedings). Within the framework of specific proceeding, a person will be identified in accordance with applicable laws and regulations (e.g.: Criminal Procedure Law[11], Criminal Law[12]; Operational Activities Law[13]), as well as data processing will take place in accordance with applicable laws and regulations (e.g.: On Processing of Personal Data in the Criminal Proceedings and Administrative Offence Proceedings[14]).

Authorizations/Notifications Required: N/A

Other: N/A

[10] Personal Data Processing Law (https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law)

[11] Criminal Procedure Law (https://likumi.lv/ta/en/en/id/107820)

[12] Criminal Law (https://likumi.lv/ta/en/en/id/88966)

[13] Operational Activities Law (https://likumi.lv/ta/en/en/id/57573)

[14] On Processing of Personal Data in the Criminal Proceedings and Administrative Offence Proceedings (https://likumi.lv/ta/en/en/id/308278-on-processing-of-personal-data-in-the-criminal-proceedings-and-administrative-offence-proceedings)

Partner: SPP | Jurisdiction: Romania

Legal Framework:

At an organizational level, the legal framework applicable to the project is seen from more perspectives:

- **Law No. 191/1998 on the organization and functioning of the Protection and Guard Service, which stipulates among other:**
  - SPP organizes and carries out, overtly or under cover, activities of gathering, checking and using the necessary intelligence, only with a view to completing the functions in the conditions established by the law;
  - carries out exchange of intelligence and cooperates with intelligence services as well as with similar departments both within the country and abroad, in order to fulfil the specific missions;
  - carries out checks through: requesting and obtaining objects, documents or official relations from public institutions; consulting specialists or experts; receiving notifications or reports; recording operative moments through technical means or personal reports;
  - puts forward requests to the prosecutor, in founded cases and in compliance with the provisions of the Criminal Procedure Code, to authorize some activities according to Law no 51/1991, for the purpose of gathering information necessary to fulfil specific missions
  - Law on prevention and combating terrorism no. 535/2004, who stipulates that Protection and Guard Service is part of National System for Preventing and Combating Terrorism
- **Ethics in scientific research, technological development and innovation activities.**
  Generally, In Romania, the activity on research projects is regulated by the following applicable laws:
  - Government Ordinance no. 57/2002, with the subsequent amendments and completions, on scientific research and technological development.
  - The National Law no. 319/2003, with the subsequent amendments and completions, regarding the status of the researcher.
  - The National Law no. 206/2004, with the subsequent amendments and completions, on good conduct in scientific research, technological development and innovation.
  - Law 206/2004 on Good Conduct in Scientific Research, Technological Development and Innovation.
  - Order 4393/2012, Regarding the Approval of The Organization and Functioning Of The National Ethics Council Of Scientific Research, Technological Development And Innovation;
  - Guidelines for Good Practice in Research.
  - Codes of Ethics for Various Research Fields.

Despite that SPP role in CounteR project as an end-user and its research activities does not fall under the incidence of applicable national legal framework for this kind of activities, internal

procedures and regulations were established in order to prove the compliance with the ethical norms and values.

There is in place a methodology regarding the project management activities, in respect to national legislation and international good practices. This methodology includes a system procedure and some operational procedures. Among these, SPP established a dedicated procedure regarding the project team, which refers to EU legislation and national Code of Ethics, Professional Deontology and Integrity in Research Activities. Every member of the project team, which is involved in research activities in H2020 projects, knows the rules, norms and values of ethics in research and applies it. There is also a written Commitment Statement to respect the ethics in research activities, which is signed by each member of CounteR project team and countersigned by the legal representative. All the Commitment Statements are kept at the project dossier from SPP and will be provided upon request. The internal Legal Department and Project Coordination and Implementation Department, are responsible for any ethics issue that should arise and the analysis of these cases will be in accordance with the legal framework mentioned above and with internal military regulations.

The military personnel of The Protection and Guard Service have all the rights and duties established for the militaries of the armed forces and they carry out their duties in the conditions established by the law and the military regulations. SPP personnel must respect the general and specific rules of ethics, behavior, integrity, respect of the society, honor and confidentiality. The main principles applicable to the national and international research projects environment formed the basis for the principles of Code of Ethics:

- LEGALITY – all activities must be compliant with the laws in force in the countries where SPP is active.
- EQUALITY, IMPARTIALITY AND FAIRNESS – all the persons are treated equally, without ethnical, nationalistic, religious, racist, political, sexual or age prejudices.
- INTEGRITY – we treat all our stakeholders as we want to be treated: fairly, respectfully and professionally.
- THE RIGHT TO A FREE OPINION – each employee has the right to express his/her point of view.
- PROFICIENCY – each employee is bound to put to good and responsible practice his/her theoretical knowledge and practical skills.
- CONFIDENTIALITY – each employee is bound to grant the security of the data and information.
- RESPECT – the consideration we give to all our protected dignitaries, colleagues and partners, to their rights and liberties, to the laws, social values, ethical and deontological regulations.
- EMPOWERMENT – SPP gives to each employee the chance to assume new responsibilities and to make important decisions.

- LOYALTY – all employees are attached to SPP values and goals, the commitment to truth and justice, responsibility for their tasks and the observance of every commitment, in respect to our organization Logo: Semper Fidelis.

- **Information access and exchange of data.**

According to the Law No. 191/1998 on the organization and functioning of the Protection and Guard Service, the activity of the Service constitutes a state secret. During its activity, the Service use unclassified and classified information, from the lowest to the highest level.

The information access and exchange of data, is regulated by the following applicable laws:

- Law No. 267 of 5 October 2005 on the ratification of the Agreement between Romania and the European Union regarding the security procedures for the exchange of classified information, signed in Bucharest on 22 April 2005. The Agreement applies to classified information or material in any form, either provided or exchanged between Romania and EU and stipulates among others, that each party shall:
  - protect and safeguard classified information subject to the Agreement provided or exchanged by the other Party;
  - ensure that classified information subject to the Agreement provided or exchanged keeps the security classification given to it by the providing Party. The receiving Party shall protect and safeguard the classified information according to the provisions set out in its own security regulations for information or material holding an equivalent security classification;
  - not use such classified information subject to the Agreement for purposes other than those established by the originator and those for which the information is provided or exchanged;
  - not disclose such classified information subject to the Agreement to third Parties, or to any EU institution or entity not mentioned in Agreement, without the prior consent of the originator.
- Government Decision no. 585/2002 - The National Standards on the Protection of Classified Information in Romania. The national standards for the protection of classified information in Romania include the implementation norms of the Law 182/2002 on the protection of classified information regarding:
  - classifications of state secret information and norms regarding the minimum protection measures within each class;
  - obligations and responsibilities of public authorities and organizations, economic entities and other public and private legal persons, as to the protection of state secret information;
  - norms regarding access to classified information, as well as, the security vetting procedure;

- general rules regarding the recording, drawing up, storage, processing, multiplication, handling, transport, transmission and destruction of state secret information;
- rules of identification and marking, compulsory inscriptions and mentions on state secret documents, on classification levels, requirements for recording the number of copies and addressees, storage terms and regime, interdictions of multiplication and circulation of documents;
- conditions for photographing, filming, cartography and execution of works of fine arts in facilities and places of special importance for the protection of state secret information;
- rules regarding the access of foreign citizens to state secret information;
- protection of classified information as part of secret industrial contracts - industrial security;
- protection of information-generating sources - INFOSEC.
- These standards establish the national system for the protection of classified information, in accordance with the national interest, with NATO criteria and recommendations, and are compulsory for all legal and natural persons handling such information.

➢ Government Decision No.781/25 July 2002 on the protection of restricted information. The document establishes the national standards for the protection of classified information in Romania, endorsed by the Government Decision no. 585/2002, shall apply accordingly, to the "secret de serviciu" (restricted) information regarding:

- classification, declassification and minimum protective measures;
- rules of accountability, drawing up, maintenance, processing, reproduction, handling, transportation, transmission and destruction;
- obligations and liabilities of the heads of authorities and public institutions, economic units and other legal persons;
- access of foreign, Romanian and other states' citizens as well as stateless individuals to classified information and to places where such activities are developed, objects are displayed or works of this category are carried out.

➢ 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. SPP recognizes that it has statutory obligations of confidentiality, to protect and respect the personal information it holds and consequently will only share personal information with a partner organization where it can be shown that:

- is processed lawfully and fairly;

- was/is collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- is adequate, relevant and not excessive in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

As a general statement, data management in SPP is done in respect with the information access and exchange of classified data regulations, which implies a higher level of procedural and security measures to protect the data collected, processed and stored.

Authorizations/Notifications Required: None

Other: During all development's stages of CounteR project, the above-mentioned regulations regarding ethics and data management will be applicable, with the following's remarks:

- during project technical development stages, since no real operational/restricted data will be used or shared with consortium partners, the provisions of the GDPR will be applicable;
- during pilot tests unfolded in Romania, if SPP will use real operational/restricted data, without sharing the data or results (except technical feedback) with other entities, the provision of Directive 2016/680 will be applicable.

Partner: BGP | Jurisdiction: Bulgaria

Legal Framework:

- Law on the Ministry of Interior
- Regulation for the implementation of the Law on The Ministry of Interior
- Penal Code, Criminal Proceedings Code
- Law on Personal Data Protection
- Similar to the competences of the other EU MS Police Authorities, BGP implements social network content monitoring within the framework its legal powers. Social networks are monitored for preventive, detective and investigative purposes.

Authorizations/Notifications Required: N/A

Other: N/A

Partner: DGSI | Jurisdiction: France

Legal Framework: *Input from this partner was not provided within submission deadline.*

Authorizations/Notifications Required: *Input from this partner was not provided within submission deadline.*

Other: *Input from this partner was not provided within submission deadline.*

3.2 International Standard

In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) which was applicable to both private and public sectors. Bearing in mind derogations to the main instrument on the basis of security, the Council of Europe adopted CoE Recommendation No. R(87)15 regulating the use of Personal Data in the Police Sector (R(87)15).

R(87)15) established an 'inalterable necessary minimum'[15] for the processing of personal data by LEAs, particularly through subjecting LEAs to the purpose specification principle. This meant that LEAs, in their role as data controllers, must process personal data only according to legitimate, specific and explicit purposes and cannot process that personal data for purposes which are not compatible with the original purposes for the processing.

This concept has been developed further and built upon within Directive 2016/680 and remains central to the regulation of processing of personal data by LEAs today.

[15] CoE's Project Group on Data Protection developed the CoE Recommendation (CJ-PD(93)48).

4 Legal Principles

This section presents the legal principles and requirements underpinning the development and piloting of the Solution, with the aim of assisting members of the Consortium, particularly technical partners and LEAs.

The lists of legal principles ('LP') set out below are simply a tool and do not purport to be a fully comprehensive solution to all privacy legal issues that may arise throughout the term of the Project, however the processing operations to be undertaken during the course of the Project must therefore be assessed in light of the list identified hereunder. As previously noted, the principle of privacy by design must be applied to the methodology of the Solution from the early stages of the Project, particularly vis-à-vis WP1: System Specifications and Architecture.

4.1 Legal Principles relevant to the development of the Project

This section identifies the salient high level legal principles as arising particularly from the GDPR that must be complied with in the course of development of the Solution by Members of the Consortium.

A. <u>Collection of Data</u>

1. **LP1** - Identify the purposes for the processing of personal data linked to the development and piloting of the Solution;
2. **LP2** – Identify the relevant category of data subjects and personal data required to fulfil the purposes identified (as per LP1);
3. **LP3 –** Identify the relevant legal basis for the processing operation and document the same;
4. **LP4 –** Collect the personal data as is necessary for the fulfilment of the purposes identified;
5. **LP6 -** Collect special categories of personal data only where absolutely necessary and where an additional legal basis for the processing of the same has been identified and documents;
6. **LP6** – Inform the data subjects, where practicable, that data has been collected and stored without their knowledge;

B. <u>Use & Storage of Data</u>

7. **LP7** - Use the data collected solely for the purposes for which it was originally collected and in accordance with the core data protection principles;
8. **LP8** - Store solely accurate data and data as are necessary to allow fulfilment of the purpose of the processing operation – subject the data to pseudonymization if possible;
9. **LP9 -** Carry out regular checks to ensure data is adequate and relevant;
10. **LP10** – Establish relevant retention periods or identify criteria that will allow determine retention of the data;
11. **LP11 -** Delete personal data in a secure manner if no longer necessary for the purposes for which they are stored, or subject the data to anonymisation;

C. **Security of Processing Operations**

12. **LP12 -** Implement privacy by design and privacy by default by implementing appropriate technical and organizational measures in an effective manner whilst integrating the necessary safeguards into the processing operations to ensure adequate protection of the rights of data subject (including encryption, access control, authentication exchange, etc.);
13. **LP13 -** Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the creation of appropriate policies and procedures that regulate data breaches;
14. **LP14 -** Notify the DPA not later than 72 hours after becoming aware of a personal data breach;
15. **LP15 -** Inform the data subject of a personal data breach where the data breach is of high risk;

D. **Rights of Data Subjects**

16. **LP16 –** Identify the relevant rights of data subjects which would be applicable to the processing operation;
17. **LP17 –** Establish mechanisms to allow data subjects to exercise their rights, as applicable;
18. **LP18 –** Establish policies and procedures to regulate the handling of exercise of data subject rights;

E. **Communication of Data**

19. **LP19** – Communicate the personal data to individuals and team members on a need-to-know basis; communication of data between members of the Consortium shall be subject to a data sharing agreement;
20. **LP20** – Where the personal data is to be transferred to a third country or international organization, ensure that an applicable data transfer mechanism is being implemented;
21. **LP21** - As controller/joint controller/processor, implement appropriate technical and organizational measure to ensure and to be able to demonstrate that processing is performed in accordance with existing legal requirements;
22. **LP22 -** As controller/joint controller, determine respective responsibilities for compliance by means of an arrangement with the controller/joint controller;
23. **LP23 -** As controller/joint controller, determine respective responsibilities for compliance by means of an arrangement with the processor;
24. **LP24 -** As processor, provide the same sufficient guarantees to implement the appropriate technical and organizational measures as if it was acting in the capacity of a controller;

F. **Record-keeping & Logging**

25. **LP25 -** Maintain a record of all categories of processing activities under its responsibility
26. **LP26 -** Keep logs for the collection, alteration, consultation, disclosure of personal data in automated processing systems, wherein such logs shall allow the possibility of establishing the justification, data and time of such operations as well as the identity of the competent authority receiving such data

G. **Consultation & Cooperation with DPAs**

27. **LP27 -** Cooperate, on request, with the DPA in the performance of its tasks

28. **LP28 -** Consult with DPA prior to processing whereby a new filing system is created

4.2 Legal Principles relevant to the implementation of Solution by LEAs

This section identifies the salient high level legal principles as arising particularly from Directive 2016/680 that must be complied with in the course of piloting and implementation of the Solution by the LEAs.

A. Collection of Data

1. **LP1 -** Collect data as is necessary for the prevention of a real danger or suppression of a specific criminal offence;
2. **LP2 -** Inform data subject, where practicable, that data has been collected and stored without his knowledge
3. **LP3 -** Collect sensitive personal data only where absolutely necessary for the purposes of a particular inquiry

B. Storage of Data

4. **LP4 -** Store solely accurate data and data as are necessary to allow fulfilment of lawful task
5. **LP5 -** Carry out regular checks to ensure data is adequate and relevant
6. **LP6 -** Delete personal data if no longer necessary for the purposes for which they are stored

C. Use of Data

7. **LP7 -** Use the data collected solely for the purposes for which it was originally collected

D. Communication of Data

8. **LP8 -** Transfer data only where the recipient has a legitimate interest, or where allowed specifically under national law or where the transfer is necessary for the prevention of a serious or imminent danger or suppression of a serious criminal offence

E. Rights of Data Subjects

9. **LP9 -** Notify the data subject to whom the data pertains that data is being held on him as soon as the object of the police activities is no longer to be prejudiced
10. **LP10 -** Provide the data subject the opportunity to confirm whether data pertaining to him/her is being processed and access same
11. **LP11 -** Provide the data subject the right to rectification or the data pertaining to him, where the right of access reveals that such data is inaccurate or incomplete
12. **LP12 -** Provide the data subject the right of erasure of data pertaining to him which is excessive, inaccurate or irrelevant

F. Security of Processing of Data

13. **LP13 -** Implement appropriate technical and organizational measures in an effective manner whilst integrating the necessary safeguards into the processing operations to ensure adequate protection of the rights of data subjects
14. **LP14 -** Notify the DPA not later than 72 hours after becoming aware of a personal data breach
15. **LP15** - Inform the data subject of a personal data breach where the data breach is of high risk

G. Data Protection Impact Assessment & Data Protection Officer

16. **LP16 -** Carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before undertaking such processing
17. **LP17 -** Appoint a data protection officer to be involved in all issues which relate to the protection of personal data

H. Record-keeping & Logging

18. **LP18 -** Maintain a record of all categories of processing activities under its responsibility
19. **LP19 -** Keep logs for the collection, alteration, consultation, disclosure of personal data in automated processing systems, wherein such logs shall allow the possibility of establishing the justification, data and time of such operations as well as the identity of the competent authority receiving such data

I. Consultation & Cooperation with DPAs

20. **LP20 -** Cooperate, on request, with the DPA in the performance of its tasks
21. **LP21 -** Consult with DPA prior to processing whereby a new filing system is created

J. Relationship between Controller, Joint Controller & Processor

22. **LP22 -** As controller/joint controller/processor, implement appropriate technical and organizational measure to ensure and to be able to demonstrate that processing is performed in accordance with existing legal requirements
23. **LP23 -** As controller/joint controller, determine respective responsibilities for compliance by means of an arrangement with the controller/joint controller
24. **LP24 -** As processor, provide the same sufficient guarantees to implement the appropriate technical and organizational measures as if it was acting in the capacity of a controller

5 Conclusions

In this document, we have defined the legal principles that underpin the development and piloting of the CounteR Solution.

In section 2, we reviewed the applicable legal framework on the processing of personal data by the Members of the Consortium during the development of the Solution, with the most relevant piece of legislation being Regulation 2016/679. With the legal framework ascertained, we assessed the relevance of the framework to the Solution and supplemented the same with the feedback on the pieces of national data protection legislation relevant to the Project provided by the Members of the Consortium that are envisaged to be involved in the processing of personal data in the development of the Solution.

In section 3, we reviewed the applicable legal framework on the processing of personal data by the LEAs forming part of the Consortium in the course of the piloting and implementation of the Solution, with the most relevant piece of legislation being Directive 2016/680. With the legal framework ascertained, we assessed the relevance of the framework to the Solution and supplemented the same with the feedback on the pieces of national data protection legislation relevant to the Project provided by the LEAs forming part of the Consortium.

In section 4, we concluded through the identification of the specific legal principles, distinguishing between the requirements throughout the development of the Project and also between the requirements in the course of the piloting and implementation of the CounteR Solution by LEAs.