Mediterranean practitioners' network & capacity building for effective response to emerging security challenges

MEDEA is a project that has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme **H2020-SEC-21-GM-2016-2017**, under grant agreement no **787111.**

Additional information about the project and the consortium can be found at www.medea-project.eu

D8.1 Establishment of DELC and requirements during the project lifetime	
Contractual Delivery Date: 08/2018	**Actual Delivery Date**: 19/10/2018
Dissemination level: Public	**Version**: 1.0

Abstract

MEDEA's Data Privacy, Ethics and Legal Committee (DELC) is a team formed by external experts on data protection, ethical, societal, legal and privacy issues that act as external – independent to the consortium. Its role is to review the project's process and results and submit short reports during the project execution period, at specific project milestones. The current deliverable attempts to describe the structure, function, and objectives of the DELC and refers to the legal framework that MEDEA should be aligned with.

Document Control - Revision History			
Issue	**Date**	**Comment**	**Author / Institution**
0.1	20/08/2018	First report draft	EUC
0.2	21/08/2018	Comments on the initial draft	Lilian Mitrou (Chair of DELC)
0.3	22/08/2018	New consolidated version	EUC
0.4	22/08/2018	Comments on version 0.3	Lilian Mitrou
0.5	29/08/2018	New consolidated version	EUC
0.6	16/10/2018	Complete DELC part, appoint members	KEMEA/EUC
0.7	18/10/2018	DELC review	Lilian Mitrou
1.1	31/01/2019	New DELC members appointed.	D. Papadaki V. Papakonstantinopoulou

Quality Control			
Issue	**Date**	**Comment**	**QA Responsible**
0.7	18/10/2018	Quality Control	KEMEA, EUC

RELEASE APPROVAL			
Issue	**Date**	**Comment**	**Responsible**
1.0	19/10/2018	Deliverable approved for submission	KEMEA
1.1	01/02/2019	Deliverable approved for re-submission	KEMEA

Statement of originality
This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Executive summary

The Consortium had an obligation to appoint an independent Data privacy, Ethics and Legal Committee (DELC) to monitor and assess the execution of the different ethical requirements within the project.

This document is the first deliverable concerning the data protection, ethics and legal reports that will be prepared under the MEDEA project; and provides information on the establishment of the Data Privacy, Ethics and Legal Committee (DELC) and the ethical standards and other EU data protection regulations that MEDEA should abide to.

Table of Contents

Table of Tables

Acronyms

Acronyms used in this document and needing a definition are included in the following table: Table 1

Table 1: Acronyms

Acronym	Definition
CoP	Community of Practitioners
DELC	Data privacy, Ethical and Legal Committee
DPIA	Data Protection Impact Assessment
GDPR	General Data protection Directive
LEA	Low Enforcement Agencies
M&BS	The Mediterranean and the Black Sea
MSRIA	Mediterranean Security Research and Innovation Agenda
NGO	Non Government Organisations
POPD	Protection of Personal Data
SC	Security Committee
TCP	Thematic Communities of Practitioners

Definitions

Concepts and terms used in this document and needing a definition are included in the following table, Table 2.

Table 2: Definitions

Concept / Term	Definition
Access rights of the individuals	Data subject's rights to access personal data held by the MEDEA consortium.
Access rights to partners/ researchers	Access to data by the staff of each partner, which is determined based on their role in the organization and on a 'need-to-know' basis.
Anonymised Information[1]	Anonymisation results from processing personal data in order to prevent identification irreversibly. Anonymised data are not considered personal data in principle, since attributing data to individuals in not possible - anonymization is designed to **irreversibly** sever the connection between the information collected and the individual. It requires the removal of the name, address and any other detail or combination of details that might result in identification. There can be no re-identification of anonymized information.
Authentication	The corroboration that a person is the one claimed.
Background	This means information and knowledge (including inventions, databases, etc.) held by the members of the MEDEA consortium prior to their accession to the Grant Agreement, as well as any intellectual property rights which are needed for carrying out the MEDEA project or for using and developing foreground.
Confidential information	Confidentiality is required as part of security for any personal data including sensitive personal and institutional information and must be given the highest level of protection against unauthorized access, modification or destruction.
Consent[2]	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's approval to agree to the processing of personal data relating to him or her.

[1] A hierarchy of preference is recommended by the Article 29 Data Protection Working Party (Opinion 5/2014 on Anonymisation Techniques), requiring, when it is possible, processing of anonymous data. If the defined scientific purpose cannot be achieved using anonymous data, pseudonymised data (or key-coded data), and only in last resort personal data may be processed. From Working Party WP 136, Opinion 4/2007 on the concept of personal data, page 26.

[2] Article 4 (11) of the GDPR

Consent [Form]	The main purpose and function of the consent (form) is the declaration of the individual/ data subject that agrees to the processing after being informed about the project and the participant's rights.
Data	Information, such as facts or numbers, collected to be examined and used aid to decision-making. Within this document data could include personal and/or sensitive personal data. In this document the terms 'data' and 'information' are synonymous.
Data Controller[3]	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
Data Processor[4]	The natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Data Subject	According to the definition of the EU General Data Protection Regulation (hereafter GDPR) an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The term *individual* can be used as a synonym for the data subject.
De-Identified Information or Pseudo anonymized information	De-identified information is information in which personal identifiers have been extracted. The most significant difference between de-identification and anonymization is that in the former an individual can be re-identify from the de-identified record using some different methods. The re-identification method may be as simple as having a confidential register assigning de-identified records back to the individual. With pseudonymization, attributing data to individuals remains possible using 'additional information' (e.g., a key or encryption code). Pseudonymised data is still considered personal data in principle. Pseudonymisation is promoted in the GDPR as one of the main methods to reduce the risks associated with processing personal data to 'help controllers and processors to meet their data protection obligations.'
Disclosure	This is the release, transfer, provision of, access to, or dissemination in any other manner of data outside the entity holding the information.
Encryption	The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

[3] Article 4(7) and (8), Articles 24, 26, 28 and 29 and Recitals (74), (79) and (81) of the GDPR
[4] Article 4(7) and (8), Articles 24, 26, 28 and 29 and Recitals (74), (79) and (81) of the GDPR

Information	In this document the terms 'data' and 'information' are synonymous.
Information Sharing Agreement	The agreement is a detailed document, which sets out precisely how the organizations involved will manage the data sharing in accordance with the purposes of the project and compliance with the legal framework. Agreements are produced where organizations specifically identify a purpose to share data across organizational boundaries.
Internal Use Only information	Includes information that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on the MEDEA consortium. Examples of this type of data include draft documents subject to internal comment before public release.
Partners	Used in the context of this document to relate to the organizations/agencies that are members of the MEDEA Consortium.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	**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**.
Public information	Information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual project partners or the MEDEA consortium as a whole.
Research Activities	These include all activities that are set out in the Description of Work of the MEDEA project.
Special categories of personal data or Sensitive Personal Data	Personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

1 Overview and key principles

1.1 Overview of MEDEA

MEDEA is a project that through its implementation aims to establish and operate a network of security practitioners, policy makers and users/ providers of security innovations across the Mediterranean and Black Sea (M&BS) countries focusing in management of migration flows, border management, surveillance and protection from cross border crime, and other Security- and disaster-related tasks. Secondly, MEDEA aims to prepare participants on how to handle emerging security challenges in the M&BS regions by identifying the current gaps, design the desirable future and define a resilient pathway in which these could be achieved. Further, MEDEA will create security technology and capabilities innovations between practitioners and innovation suppliers and will establish and annually update the Mediterranean Security Research and Innovation Agenda (MSRIA), that identifies areas where security & defense research is needed and the establishment of recommendations for European Security & Defence technology investments.

Within MEDEA four Communities of Practitioners (CoPs) are proposed, dealing with the critical threats and risks identified in the M&BS region.

i) Thematic Communities of Practitioners (TCP) on “Management of Migration Flows and Asylum seekers.”
ii) TCP on “Border management and Surveillance.”
iii) TCP on “Cross-border organized crime and terrorism.”
iv) TCP on “Natural hazards and technological accidents.”

For each Thematic area, there is a dedicated Work Package (starting from WP2 to WP5). In each one, the first Task is to prepare a set of scenarios, then based on some criteria there will be a selection of only some scenarios that will form the basis on which identification of gaps in the existing procedure, policies, practices, and technology will occur.

Then these will be delivered to the Security Committee (appointed in [AD.1]) that will be in charge of reviewing Project deliverables, in view of deciding about their dissemination in the public domain, possibly after a suitable screening of sensitive information. Subsequently, DELC will identify if any privacy issues are present, and will suggest privacy by design elements that should be taken into consideration by the technical developers and researchers at a later stage. The MEDEA Network and the CoPs will interact with the external DELC and will jointly and continuously assess the ethical and legal aspects, and the impact of the methodologies and solutions developed within the project.

All MEDEA partners have agreed to protect citizens’ data and privacy, and therefore each consortium partner has agreed to comply with all respective EU regulations and main Data Protection Principles,5 throughout the lifecycle of MEDEA project. MEDEA will not collect,

[5] All principles with which MEDEA partners have agreed to comply are clearly stated in Page 106 of 137 of Part B of the Grant Agreement [AD.1]

analyze or store any personal data within MEDEA Network activities or scenarios development as stated in [AD.2].

In the unlikely event that any personal data are collected during the MEDEA project, they will be securely stored and retained only for the lifetime of the project, namely until the 31st May 2023 and they will be securely deleted on that date. Hardcopies of the consent forms will be securely stored in lockable storage cabinets and will shredded via paper shredding machine by the end of the project.

Any data collected will not be used outside the project scope.

In the unlikely event where, further processing of the previously collected personal data is required, a new consent is required.

1.1.1 Pilots/ Demonstrations

Moreover, selected capabilities that are of high interest to the practitioners will be tested in a real-world environment (in TCP1, TCP2 and TCP4), in the MEDEA demonstration sites. During these demonstrations and the table top exercise (for TCP3) between practitioners, ***no personal data will be acquired***.

1.1.2 Surveys/ interviews/ questionnaires

Data collected through automated mechanisms or surveys/interviews/ questionnaires from the TCP participants will only be kept for the MEDEA project and only for the duration of the research period. The questionnaires that will be designed to record the Community of Practitioners' opinions will be *anonymous*. No personal data will be processed, and in any case, fully anonymized engineered data will be circulated to the rest of the consortium partners for metadata scientific research analysis.

1.1.3 Third parties data transfer

The data that will be collected throughout the project will not be shared with any third party.

1.1.4 Online Collaborative platform

The Collaborative platform will be developed aiming to allow more efficient dissemination of material and the scenarios, to facilitate the cooperation amongst the members, exchange ideas and opinions on MEDEA related matters for further processing and decision making. For this platform user accounts will be created – asking for personal user data to fulfill registration (e.g., Name, Surname, email, etc). All personal data that will be collected will only be used for this purpose and will be stored on KEMEA's servers and will be handled according to the relative requirements of GDPR. In case of members' participation and interaction with the collaboration platform, an 'opt in/opt-out' functionality will be available. The MEDEA consortium has identified that all Network activities will be executed with the Network participants, through the online collaborative platform that will be developed, as well as, collection, processing, and storage of personal, but not sensitive, data.

1.2 Project Requirements

1.2.1 Data protection by design as a principal choice/ approach

Concerning the requirements of the project, the GDPR requirement to consider data privacy at the initial design stages of a project, as well as throughout the lifecycle of the relevant data processing, will be implemented. In the following DELC deliverables, the rules that the partners should comply with and the requirements that derive thereof will be clearly stated. In this context, the Partners should embed these privacy and data protection principles in the design of applications.

A primary goal is to roll-out and adopt a privacy-by-design approach, meaning that the technical solutions will be conceived and designed from the outset, bearing in mind legal constraints and complying thereto. The project conceives security and privacy by design as procedure/tool seeking to embed legal requirements into the entire life cycle of the project, from the early research and design stage to its deployment, use, and ultimate disposal.

Partners are aware that solutions and applications proposed through MEDEA need a thorough ethical and legal assessment that demands intervention and monitoring at several stages of the project.

In this context it has been recommended that to conduct a privacy impact assessment (kind / scope / categories of the information – purposes / uses / retention period etc.) for assessing the impacts on privacy and taking remedial actions are necessary in order to identify severity levels and avoid, mitigate or minimize adverse impacts and risks.

1.2.2 Data Protection Impact Assessment (DPIA)

The project requirements may raise the possibility to carry out a **Data Protection Impact Assessment (DPIA)**. In accordance with the features set by the GDPR (Article 35(7), and recitals 84 and 90), i.e., it will consist at a minimum by

a) “a description of the envisaged processing operations and the purposes of the processing”;

b) “an assessment of the necessity and proportionality of the processing”;

c) “an assessment of the risks to the rights and freedoms of data subjects”; -

d) “the measures envisaged to “address the risks” and “demonstrate compliance” as required by the accountability principle.

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is “likely to result in a high risk to the rights and freedoms of natural persons” (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)).

Data protection impact assessment under GDPR: Article 35 of the GDPR requires that controllers (i.e., entities determining the purposes and means of personal data processing) carry out a data protection impact assessment in situations ‘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'.[6] Article 35 requires to carry out a DPIAs in situations which entail:[6]

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which are based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data (e.g., revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited) or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

The DELC aims to ensure that the steps recommended during the DPIA are implemented and that the PIA will continuously be used throughout the project's lifecycle. The DELC will help the consortium when conducting the DPIA and is responsible for highlighting privacy, ethical and legal risks based on their area of expertise and thereon provide external consultation and guidelines to the MEDEA consortium, to ensure compliance with the relevant legal framework and contribute to identification and mitigation of risks.

1.3 Ethical Principles and Data Protection regulations in MEDEA

The MEDEA consortium is committed to the ethical conduct of the project's research activities which meets both national and international ethical standards. Whenever information and communication technologies (ICTs) are involved, it is necessary to take into account one fundamental right in particular: the right to data protection. This is a fundamental right enshrined in Article 8 of the EU Charter of Fundamental Rights. European and national data protection laws and other regulations that govern the processing of personal data constitute the backbone of the project (See Section 3). Widely-accepted ethical standards consider proper governance arrangements as essential to ensure that any risks to the lawful and ethical conduct of the project are identified and minimized so that they do not compromise legal and ethical standards.

1.4 Guidance to participants on the procedures to follow

Guidance for helping participants in identifying and contacting the responsible partner will be provided by the DELC on a case by case basis. As MEDEA stands, we believe that the only responsible agencies that may be needed to contact are the national Data Protection authorities (DPAs) since only personal data for the online collaborative platform (Section 3.1) will be collected and processed. A list of this competent partner per participating member state will be created. This plan would be approved by DELC members and will be the output of interactions between DELC and MEDEA members.

[6] General Data Protection Regulation, Article 35

1.5 The rationale of The MEDEA DELC

The MEDEA consortium will ensure that its principles for the lawful and ethical conduct of the project's research activities are adhered to through its DELC. The DELC is a group of two independent recognized academics experts, external to the project, that will act alternatively as chairs, and three associated with the project, distinguished professionals in Data Privacy, Ethics and Legal domains. The two experts will supervise the recommendations and guidance provided by the three associated DELC members and will be responsible for ensuring MEDEA's compliance with active EU directives and recommendations.

The DELC will review the project's activities and outputs and formally assess if they meet ethical standards and data protection requirements on a six months basis. The DELC will have the power to safeguard that data gathering procedures complies with General Data Protection Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive (EU) 2016/680 Of The European Parliament And Of The Council of 27 April 2016 and the respective national legislation. The Committee will provide guidance to the project on issues relating to national and EU legislative requirements for the use of personal data and other legal and/or ethical implications that may arise throughout the duration of the project, such as dual-use and misuse. Its ultimate goal is to promote high ethical standards for the duration of the MEDEA project and ensure that the research conducted by the MEDEA project is classed as ethically sound. The DELC will monitor compliance with the project requirements regarding ethical, privacy and data protection issues throughout the project lifetime and will assess the sensitivity of all deliverables before any publication and will review progress regularly assuring constantly an appropriate classification level.

2 MEDEA DELC structure

2.1 Committee members

The DELC will be chaired alternatively by Professors Dr. Lilian Mitrou and Dr. Eleni-Tatiani Synodinou who will set the Ethics Agenda, the meeting protocols and records projects issues, consortium decisions and action with regards to Ethics, Data Protection, and Legal issues.

Dr. Lilian Mitrou (Female), is Professor at the University of the Aegean-Greece (Department of Information and Communication Systems Engineering) and Visiting Professor at the Athens University of Economics and Business and at the University of Piraeus (Postgraduate Studies Programs). She teaches information law and data protection law. L. Mitrou holds a Ph.D. in Data Protection (University of Frankfurt- Germany). She was Member of the Hellenic Data Protection Authority (1999-2003). From 1999 till 2001 she was representative of the Hellenic Data Protection Authority at the Art. 29 Data Protection Working Group and from 2001-2004 national representative in the EC- Committee on the Protection of Individuals with regard to the Processing of Personal Data. During the Greek Presidency of the Council of EU (2014), she has served as Chair of DAPIX (Working Group on Information Exchange and Data Protection). From 1997 till now she served as member/ chair of many Committees working on law proposals in the fields of privacy and data protection, communications law, e-government, etc. Since June 2016 she chairs the Committee charged with the implementation/transposition of the new European Data Protection Framework (Regulation 2016/679/ EU and Directive 2016/680/EU) into national law. Her professional experience includes senior consulting and researcher/ expert positions in a number of private and public institutions and projects on national and international level. Her research interests include: Privacy and Data Protection, e-Government services, Internet Law, Cybercrime and Digital Forensics, Responsible Research and Innovation. L. Mitrou published books, chapters in books and many journal and conference papers (in English, German and Greek).

Dr. Eleni-Tatiani Synodinou (Female) is an Associate Professor at the University of Cyprus. Tatiani Synodinou worked as scientific collaborator with teaching duties at the Faculty of Law of Aristotle University of Thessaloniki (2001-2004) and as a full time Visiting lecturer the Interdisciplinary postgraduate program of “Informatics and Management” of the Aristotle University of Thessaloniki. She has been a member of the Bar Association of Thessaloniki since 2000. She has worked as a short time expert to EU twinning projects and was a member of the e-business Advisory Board for the study “Intellectual Property for ICT producing SMEs” in the context of the 'Sectoral e-Business Watch' 2007-2008. She is a case law reporter for “Kluwer Law International” to the legal database «Kluwer EU IP Cases» and a contributor to Kluwer Copyright Blog. She has also been a National expert for many projects and EU studies, such as the Public Domain Calculator project, European Connect (www.outofcopyright.eu), Study on sport's organizer rights in the EU, Asser Institute-IVIR 2014, etc.). She is the Chair of the Ethics Committee of the project Mandola (Monitoring and Detecting On line Hate Speech). She has been the main organizer of the International Conference “Towards a European Copyright Code?” which was held on April 14-15, 2011 at the University of Cyprus and co-organiser of the international conference REDA 2015 -Regulation and Enforcement in the Internet Era, (Nicosia, 5-6 November 2015).

2.2 Selection and formation of the DELC

Three lawyers will assist the DELC committee with their tasks. The members of the DELC were selected by the MEDEA consortium based on their expertise, experience, and knowledge in the fields of:

- Conducting research (and associated ethical standards)
- Data protection
- Privacy by design
- Data protection by design

The following are the appointed members of DELC:

Vasiliki Papakonstantinopoulou (Female) studied Law at the of Aristotle University of Thessaloniki School of Law from1997 till 2001. In 2004 she completed her postgraduate studies and obtained a master's degree on Public Law. Vasiliki Papakonstantinopoulou holds an LLM on Information Technology Media and E Commerce Law (University of Essex UK). From March 2002 till October 2003, she worked as a practicing lawyer at Piraeus Bank of Thessaloniki and then as a practicing lawyer of the Legal Council of the State from October 2004 till September 2005. Since 2005, she works as a lawyer – (member of the Athens Bar Association), and she is been dealing mainly with labour, public law and personal data protection law. From 2017 onwards, she participates in GPDR's Compliance Groups and has been appointed as DPO for occupational Pension Funds.

Dimitra Papadaki (Female) is a lawyer (Athens Bar Association) who holds a Bachelor of Laws from Athens School of Law (National and Kapodistrian University of Athens). Ms Papadaki holds a Master of Laws in International Legal Studies, with specialization in Private International and Comparative Law from Athens School of Law. She also holds a Master of Laws in International Human Rights Law from the University of Essex UK. Her studies have provided her with the background to deal with issues regarding the interaction of European Union Regulations with international and national legislation and the protection of the right to privacy. She had served as a researcher for the Human Rights Clinic of the University of Essex, and in this capacity, she had been conducting research with human participants, had been applying for and accomplishing ethical approval from the respective Ethics Committees. Ms Papadaki serves KEMEA as a Research Associate.

Christiana Markou (Female) is a scientific collaborator in the University of Nicosia and a law lecturer in the European University Cyprus and Open University of Cyprus. Christiana teaches European Consumer Law, European Private International Law, Special Issues of EU Internal Market Law and Legal Research Methodology. She practices law from 2001 onwards. Christiana obtained a LL.B and LL.M in European, Commercial and International Law from University of Sheffield, UK and a PhD from University of Lancaster, UK in the EU consumer and data protection/privacy law.

2.3 Scope

The Committee will provide guidance and advice to Management and Work Package leaders on ethical, privacy, and personal data processing issues whenever required.

The Committee will provide guidance in the development of a transparent and robust methodology regarding the collection, storage, processing, exchange, analysis and manipulation of personal data, if any, and will assess the implementation of this methodology for the duration of the project.

It must be noted that the DELC does not substitute any national or local ethics committee. The Committee instead plays a supporting role to such national committees by reviewing and approving/rejecting all procedures involving human subjects/data; ensuring that each partner strictly adheres to the highest privacy and ethical standards.

3 MEDEA framework for Data Protection

3.1 European Legal Framework

Currently, Europe has one of the most comprehensive frameworks governing privacy and data protection. The MEDEA consortium has carefully considered all respective EU legislation, international conventions, and declarations pertaining to:

- The European Convention On Human Rights
- The EU Charter of Fundamental Rights and Freedoms
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108. The original convention of 1981 has been revised and approved on 18/5/2018[7].
- The General Data Protection Regulation (GDPR) (EU) 2016/679.
- 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.

3.1.1 The European Convention On Human Rights

The right of an individual to a private life is acknowledged as a fundamental right enshrined in Article 8 of the European Convention on Human Rights (ECHR). It includes four discrete areas: private life, family life, home, and correspondence. The Court has applied a broad definition of the notion of private life in Article 8 of the ECHR, extending it far beyond the walls of the private house and the intimate sphere. In this view 'private life' embraces the development of interpersonal relationships and protects not only the domestic sphere but also (data relating to) certain facts occurring in the public sphere and protection of personal data. The European Court of Human Rights has perceived and construed Art. 8 broadly to protect individuals against the collection and processing of personal information, even if that information is considered commonplace or is already widely available.

3.1.2 EU Charter of Fundamental Rights and Freedoms

The Charter of Fundamental Rights of the European Union has embedded both an individual's "right to respect for his or her private and family life and correspondence" (Article 7), which is modelled after the ECHR and "the right to the protection of personal data" (Article 8), which is consolidated thereby as a new, autonomous fundamental right. Moreover, Article 8 of the Charter lays down the components of this "new right", which at the same time constitute data processing criteria, i.e., fair processing, purpose limitation, consent of the data subject, access right, independent authority.

[7] Council of Europe Explanatory Report of Convention 108.

All European countries are required to abide by the Charter, as it has been given a legally binding value for EU institutions and bodies as well as for Member States with regards to the implementation of Union law.

3.1.3 Council Of Europe Convention 108

Convention 108 is the first international legally binding instrument concerned with data protection. It applies to all data processing conducted by both private and public entities and safeguards individuals against any abuses that may arise from the collection and processing of personal data. Convention 108 lays down several principles, namely, that collection and automatic processing of data must be fair and lawful; data should be stored for specified legitimate purposes and not used for ends at odds with these purposes; data should not be retained for longer than is necessary; data must be adequate, relevant and not excessive (proportionality) as well as accurate (principles of quality). The Convention also outlaws the processing of "sensitive" data (e.g. race, politics, health, religion, sexual life, criminal record, etc.), without the proper legal safeguards and imposes certain restrictions on the trans-border flow of personal data to third-party States where legal regulation does not provide the same level of protection. The original convention of 1981 has been revised and approved on 18/5/2018.

3.1.4 The General Data Protection Regulation and Directive (EU) 2016/680

The EU Data Protection Regulation 2016/679 requires that Member States ensure the rights and freedoms of individuals with regard to the processing of personal data, and in particular their right to privacy. It further reinforces the fundamental rights laid down in Articles 7 and 8 of the Charter of fundamental rights of the European Union (see 5.1.2). Its provisions include data quality, special categories of processing, the rights of data subjects, confidentiality, security, liability and sanctions, codes of conduct and supervisory authorities.

Of particular significance to the MEDEA, consortium is Article 78 of the GDPR which requires data controllers to protect personal data against a variety of risks through the adoption of appropriate technical and organizational controls. Specifically, these controls must be incorporated into the design of the processing system and also the processing itself. This means that security cannot simply be added on to data systems but must be built in; this is known as “privacy-by-design.”

GDPR is applicable in the context of the research project while the Directive (EU) 2016/680 will be considered while designing the security technology and capabilities innovations.

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 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, OJ L119/89. Article 53 of the Directive (EU) 2016/680 refers explicitly that in order to protect the rights of the data subjects with regard to the processing of personal data, the appropriate organizational and technical measures should be in place and should be implemented to adhere in particular to the principles of data protection by design and data protection by default.

3.1.5 Keywords for The MEDEA Consortium

It is clear from the previous sections (3.1.1 to 3.1.4) that the EU has enacted several provisions that mutually reinforce each other to safeguard an individual's privacy and ensure data protection. Several keywords and key terms emerge throughout these provisions that the MEDEA consortium is advised to consider at all times throughout the project's lifetime (including in the design stages):

3.1.5.1 Dignity and Privacy

In each phase of the research project the rights and freedoms of the data subject and mainly his/her dignity and privacy, will be respected and protected according to the law and the ethical guidelines.

3.1.5.2 Consent

No person/data subject will participate without his/her legally effective explicit and informed consent. The researcher shall ask for such consent only under circumstances that give to the prospective subject or the representative the possibility to consider sufficiently whether or not to participate, minimizing, therefore, the possibility of coercion or undue influence. The information that is given to the subject or the representative shall be in a language understandable to the subject or the representative.

The information given must include:

- A statement concerning the research purposes of the study, an explanation of the specific purposes of the research as well as a description of the procedures to be followed.
- A statement that all personal data will be de-identified before their use within the research project.
- A description of any benefits to the subject or to others which may reasonably be expected from the research.
- An indication of the contact person for answers concerning pertinent questions about the research and research subjects' rights.
- A statement that participation is voluntary, that refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and that the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.
- A statement that a withdrawal from the research does not have any consequence or penalty on benefits.
- The list of the partners of the Project, who may have access to the data subject's data.
- A statement about the length of the anonymized data retention period, depending on consent given only for the project goals or also for general anonymized database availability at the end of the project.

3.1.5.3 Purpose

Data controllers and data processors will collect, retain and use the provided data only for the explicit, legitimate, clearly specified and documented purpose(s) of this project as laid down in the Description of Work of the project.

Data may not be processed for purposes which are not compatible with the project's purposes and/or further (re)used for other purpose(s) that is/are not covered by the consent.

3.1.5.4 Data minimization

Only personal data that are adequate, relevant and limited to the minimum necessary in relation to the purposes of the project shall be collected and processed. Personal data will be kept in a form which permits direct or indirect identification of data subjects for no longer than is necessary for the purposes of the project.

If personal data is no longer necessary, it will be erased/destroyed unless (and to the extent) that it is necessary for the documentation of the research.

3.1.5.5 Accuracy of data

Data collected and processed for the purposes of the project have to be accurate, reliable and kept up to date. The Data Controller is responsible for the quality of data and the fair and transparent processing of data and has to ensure that data will be corrected, revised and/or updated when requested by a data subject or deemed to be necessary as a result of regular audits and reviews.

3.1.5.6 Data subjects' rights

The underpinning principle of research is that the rights of the individual take priority over the research needs. Persons involved will not be disadvantaged if they refuse to let researchers collect their data. They have the right to withdraw their consent and stop participating in the research project at any time without any consequences or loss of benefits. The data controller will ensure that data subjects may exercise their right to access to their data collected and stored for the purposes of the project as well as the right to object to the further processing and/or to request rectification or erasure of their data. In case that a data subject is exercising these rights, the data controller will notify the data processors who have to act respectively.

3.1.5.7 Responsibilities

Researchers must ensure that data subjects understand the implications of taking part and consenting to the collection of their data. Data collection must be fair and transparent for the persons concerned. Researchers involved in data collection and processing must ensure that data are accurate and reliable.

Researchers acting as data processors are responsible and accountable for complying with these guidelines, the national law and the specific instructions of the data controller and they are bound by the confidentiality obligation.

3.1.5.8 Access to data and transfer of data

Researchers acting as data processors will have access only to data that they are specifically mandated and/or authorized to use.

Access to any database holding personal data is restricted to data processors who are specifically mandated / authorized to have access and process personal data for the purposes of the project

Data may be transferred to data processors only after the approval of the data controller. Neither the data controller nor the data processors are allowed to transfer, to disclose or to make available data to third parties outside the Consortium.

3.1.5.9 Security

The Data Controller and the Data Processors (Researchers and the organisations in which they are situated) are responsible for data security according to these guidelines and having regard to the data they deal with they will adopt and implement all the appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

If the access or the exchange of data involves their transmission over a network the data controller and the data processors will take all the appropriate measures to transmit the data via a secured network and/or by a secured procedure in order to prevent unauthorized access and interference to the network or to the data. Data security will be preserved through anonymization, encryption, and regulation of the medium of transfer.

Each consortium member will be responsible for data security within its own organization, according to the national law, respective codes of conduct and professional standards as well as the guidelines approved within the consortium for data treatment and data security.

3.1.5.10 Anonymisation

In order to protect privacy and the right to data protection, data gathered containing any personal information will be anonymized. This anonymization is carried out under the responsibility of the data controller just after their collection and in any case before the further processing of data by data processors who hence will have access only to de-identified data.

When data will be inserted in the MEDEA database, they will be completely de-identified, assigning a unique ID that will allow strictly within the Data Controller the re-identification and only for the purposes of Data subjects' rights.

3.1.5.11 Accountability

The data controller is accountable for compliance with the law and these guidelines and is responsible for taking the necessary technical and organizational measures and the accuracy and reliability ("data quality") of the data collected and distributed. The Data Controller must be able to demonstrate compliance with the law and the principles governing data processing.

3.2 Privacy

Privacy is about the right of an individual to be let alone and to lead a life free from unwanted or unwarranted intrusion or interference in their private life and affairs. As the research activities of MEDEA will not impact on the physical privacy of any individuals the focus of the Committee will be on data or informational privacy.

Informational privacy responds to the requirement that everyone should be in control of the information concerning them so as to formulate conceptions of self, values, preferences, goals and to protect their life choices from public control, social disgrace or objectification. Informational privacy offers safeguards to preserve an underlying capacity for autonomous

decision and choice-making. Data privacy is the ability of an individual to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Data privacy involves the right of an individual to expect that personal information collected about them will be processed securely and will not be distributed in any form without their written consent, unless there is an exception provided by law.

Data protection is the instrument for safeguarding data privacy.

4 Conclusions

The current deliverable aims to draw the Data Privacy, Ethics and Law Committee's course of action, pinpoint the relevant EU laws that should be taken into consideration for the MEDEA project. It also sets the requirements that should be met during the project lifetime to ensure data protection and privacy. MEDEA project aims to identify the gaps in the existing technology and the practices that will be delivered as an output of the project, and then DELC will suggest some privacy by design and data protection by design issues that technical developers and researchers will need to follow during the project lifetime.

5 References

1. Council of Europe. (1981). Explanatory Report of Convention for the protection of individuals with regard to automatic processing of personal data. *European Treaty Series*, *679*(108), 14. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

2. Council of Europe. (1950). *European Convention on Human Rights*. Retrieved from http://www.echr.coe.int/Documents/Convention_ENG.pdf

3. Council of Europe (COE). (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *European Treaty Series*, (108), 1–9. Retrieved from https://rm.coe.int/1680078b37

4. Data Protection Working Party. (2014). *ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 05 / 2014 on Anonymisation Techniques Adopted on 10 April 2014*. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

5. European Commission. (2000). The Charter of Fundamental Rights of the European Union. *Official Journal of the European Communities*, *C*(364), 1–22. https://doi.org/10.1108/03090550310770974

6. European Commission. (2018). Proposal for a Council Decision authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No, *0237*(108).

7. European Convention on Human Rights. (2010). Convention for the Protection of Human Rights and Fundamental Freedoms, *5*(5), 13. https://doi.org/10.2139/ssrn.1809643

8. European Court of Human Rights. (2002). The right to liberty and security of the person - A guide to the implementation of Article 5 of the European Convention on Human Rights. *Human Rights Handbooks*, (5). https://doi.org/10.1086/206470

9. European Parliament, C. 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 (GDP (2016). European Parliament and of the Council. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

10. European Parliament, & The Council. (2016). Directive 2016/680 of the European Parliament and the Council 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 crimi. *Official Journal of the European Union*, *2014*(April), L 119/89-L 119/131. https://doi.org/L 102/15

5.1 Applicable documents

The following documents, of the exact issue shown, form part of this document to the extent specified herein. Applicable documents are those referenced in the Grant Agreement or approved by the Approval Authority. They are referenced in this document in the form [AD.X]:

Table 3: Applicable Documentation

Ref	Title	Date
[AD.3]	GRANT AGREEMENT NUMBER — 787111 — MEDEA	15/05/2018
[AD.4]	D9.2 lists all DPOs from each partner	19/10/2018
[AD.5]	D9.5 mentions the Security committee – it gives recommendations that will be passed into DELC	17/10/2018

6 Annex I - Guidance On Consent Forms

Consent forms must:

1. Be easily accessible and easy to understand, with **clear** and **plain** language used.
2. Provide information to the data subjects on the identity and contact details of the data controller and, where applicable, of the controller's representative.
3. Provide information on the purposes of the data processing as well as the legal basis for the processing.
4. Provide information on the risks, rules, safeguards and rights in relation to the processing of personal data and how a data subject can exercise their rights in relation to such processing.
5. Provide information on the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
6. Provide information on the rights of the data subject including the right to withdraw consent at any time; the right to request from the controller access to and rectification or erasure of personal data or restriction of processing; the right to lodge a complaint with a supervisory authority.

They must elicit:

- Consent to participate in the MEDEA project.
- Consent for partner agencies to share both information and documentation across partner agencies, in order to implement the necessary tasks required for the project
- Consent for information to be stored by the MEDEA consortium/MEDEA partner
- Consent to be contacted by partner agencies from the MEDEA consortium, for the purpose of the project.
- Consent to the right to withdraw from the study at any point.