This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293

IMMERSE. INTERACT. INVESTIGATE.

INFINITY

D2.3 Analysis of relevant legal, societal and ethical framework

DISSEMINATION LEVEL PUBLIC

D2.3 Analysis of relevant legal, societal and ethical framework

PROJECT INFORMATION

Grant Agreement No	883293
Acronym	INFINITY
Name	IMMERSE. INTERACT. INVESTIGATE.
Topic	SU-FCT-02-2018-2019-2020
Funding Scheme	Research and Innovation Action
Start Date	01/06/2020
Duration	36 months
Coordinator	Airbus Defence and Space SAS

DELIVERABLE INFORMATION

Work Package	WP2 Analysis of the societal, legal, ethical and well-being considerations for Infinity		
Deliverable	D2.3 Analysis of relevant legal, societal and ethical framework		
Contractual Delivery Date	28/02/2021		
Actual Delivery Date	15/03/2021		
Type	R - Report		
Dissemination Level	Public		
Lead Beneficiary	UNIVIE		
Main Author (s)	Nikolaus Forgo	UNIVIE	
	Max Koenigseder	UNIVIE	
	Thomas Por	UNIVIE	
Contributing Author (s)	Author Name	Organisation	
Reviewers	Reviewer Name	Organisation	Date
	Philippe Chrobocinski	ADS	15/03/2021
	Ourania Theodosiadou	CERTH	08/03/2021

REVISION HISTORY

Version	Author Name(s)	Organisation	Date	Contribution
0.1	Nikolaus Forgo, Thomas Por, Max Königseder	UNIVIE	16.02.2021	First version
0.1	David Pannocchia	CENTRIC	22.09.2020	SHIELD Framework
0.2	Max Königseder	UNIVIE	26.02.2021	Section 4.4.3
0.3	Thomas Por	UNIVIE	26.02.2021	Minor adjustments
0.4	Stephanie Philippe, Morgane Burgues	MANZA	01.03.2021	Corrections
0.5	Rodolphe Roques-Couchot	EUROPOL	01.03.2021	Europol Regulation corrections
1.0	Thomas Por, Max Königseder	UNIVIE	05.03.2021	Final version

DISCLAIMER

EXECUTIVE SUMMARY

This report, D2.3, is the interim result of Task 2.3 and provides an **initial analysis of the relevant legal, societal and ethical framework**. This report will contribute to the overarching aim of WP2 to provide legal and ethical analysis in relation to activities taking place during the project, as well as for post-project end use of the system by LEAs in real-life scenarios. This report will provide a legal analysis of these distinct yet interconnected settings.

For the course of the project a novel framework developed by CENTRIC will be applied to enhance the compliance of the project to the legal, ethical and data considerations outlined in this report. The SHIELD (Security, Human-centred, Integrity, Ethical, Legal and Data) Framework is designed specifically for research and development of advanced security solutions that utilise avant-garde technologies such as AI, big data and XR, amongst others.

This deliverable constitutes a reference document for all partners on the applicable legal, ethical and regulatory framework. Issues which may arise from field use of INFINITY will be examined, along with user perspectives identified through a partner questionnaire. As part of its analysis, this deliverable will take into consideration both Union and national legislation, including EU fundamental rights and primary law, secondary EU law, and the national law of EU Member States.

Particularly, the GDPR and law enforcement directive, as well as the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union will be analysed. Additionally, the Europol Regulation and its implementing rules for any processing operations upon personal data carried out by Europol will also be examined within that document. Focus will be paid to the relevant terminology and principles of those data protection frameworks that are inherent to these legislations.

The aim of this report is twofold. Firstly, to establish the framework in which the capabilities can be developed in the project and on the other hand already give a first outlook in which framework INFINITY can be used operationally. The initial societal impact will also be examined, focusing primarily but not exclusively on data protection issues.

In its entirety, D2.3 can be viewed as a reference document for the legal issues and societal impact as connected to the processes which will take place both within the INFINITY project (in connection with D1.4), and outside the project upon the completion and subsequent application of the INFINITY solution.

ABBREVIATIONS

AI	Artificial Intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPA	Data Protection Authorities
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ER	Europol Regulation
FRA	Fundamental Rights Agency
PET	Privacy-enhancing technologies
GDPR	General Data Protection Regulation
I^3CE	Investigative Immersive and Interactive Collaboration Environment
ICO	Information Commissioner's Office
LEAs	Law Enforcement Agencies
LED	Law Enforcement Directive
MS	Member State
SHIELD	Security, Human-centred, Integrity, Ethical, Legal and Data
TFEU	Treaty on the Functioning of the European Union
VR	Virtual Reality
XR	Extended Reality

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

INFINITY's ambition is to become a flagship project against society's most pressing cybercriminal, terrorist and hybrid threats. The overarching aim of INFINITY is to develop an integrated solution that revolutionizes data-driven investigations and propel LEAs ahead of traditional and evolving complex, hybrid and transnational threats. To achieve its objectives INFINITY will synthesize the latest innovations in virtual and augmented reality, artificial intelligence and machine learning with big data and visual analytics. Investigators and analysts will be equipped with cutting-edge tools to acquire, process, visualise and act upon the enormous quantities of data they are faced with every day.[1] Section 1 will give a brief overview of this deliverable, how the deliverable is positioned within the project, describe the connected legal deliverables und provide a timeline for these and introduces the structure of this report.

1.1 OVERVIEW

This report, D2.3 'Analysis of relevant legal, societal and ethical framework' is the interim result of T2.3.[2] In its entirety, D2.3 can be viewed as a reference document for legal, ethical and societal considerations connected to the processes which will take place both within the INFINITY project and outside the project upon the completion and subsequent application of the INFINITY solution. As part of its analysis, this deliverable will take into consideration both Union and national legislation, including EU fundamental rights and primary law, secondary EU law, and the national law of EU Member States.

1.2 DELIVERABLE POSITIONING

This Report is embedded in a multitude of tasks concerning ethical, legal and data protection issues within INFINITY. D2.3 must be read together with the deliverables of WP11 defining the ethics requirements set out by the EC after its ethics review, the Data Management Plan (T1.5) (a first version is available since M6) and especially all subsequent deliverables of WP2 which will further establish and monitor not only the legal and ethical requirements but also the wider societal impacts of the INFINITY solution in detail. A societal impact report will also be developed within D1.7. Even though the legal deliverables are distinct from the technical deliverables, they aim to impact and shape the technical architecture at the design and development stage of the solution. This way we can ensure that the solution will not only be deployable in a legally compliant way but also include PET features wherever feasible.

1.2.1 LEGAL DELIVERABLES AND WP2

This deliverable is one out of four interrelated deliverables on legal matters of the project (D1.4, D2.3, D2.4 and D2.5). D1.4 has elaborated the basic concepts of data protection and ethical research that all partners need to adhere to and provided guidelines for their applicability within the projects research context. Additionally, the deliverable dealt with the ethical dimensions of innovation and research and special considerations regarding the protection of personal data. D1.4 has been delivered in M4. This report, D2.3, provides the interim legal, ethical and societal framework that will be relevant for INFINITY both in terms of innovation and deployment of the solution. D2.3 will act as a legal assistance tool for partners on legal framework requirements in their development and use of the INFINITY solution. D2.3 provides the legal framework analysis to assist in the reading of D2.4, which will report on the risk assessment and will elaborate how the proposed application INFINITY can best comply with the framework developed within this report. The process of continuous monitoring of legal and ethical issues will be addressed within all of the WP2

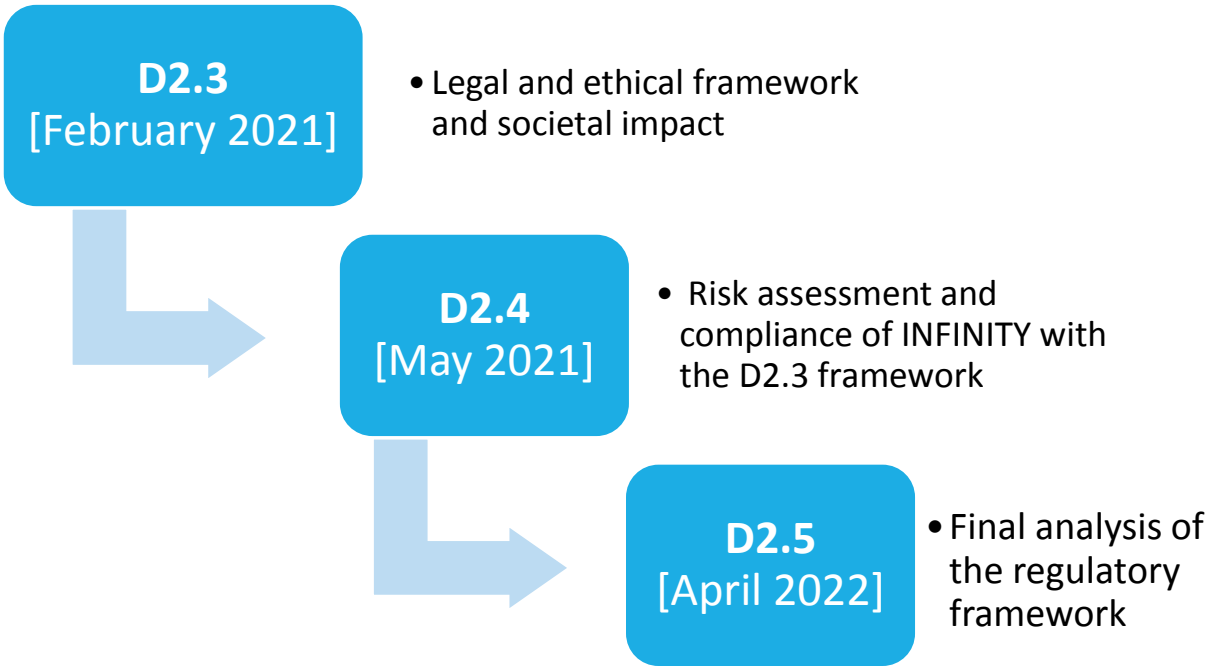
[1] INFINITY Grant Agreement (883293) page 88.
[2] INFINITY Grant Agreement (883293) page 102.

deliverables. This process will result in the final analysis of the regulatory framework in M23 mid-term of the project. D2.5 will be built upon D2.3 and D2.4 and provide the final analysis of relevant legal, ethical and regulatory framework and societal impact, especially reflecting on the use cases, the technical developments and progress. D2.5 will finalise the WP2 efforts by providing an analysis applicable to the post project compatibility. The document presents the results of the analysis of INFINITY framework to issue recommendations mid-term of the project.

1.2.2 WP2 TIMELINE

The process and timing of the legal deliverables within WP2 are illustrated below.

Figure 1 WP2 Deliverable timeline



1.3 DELIVERABLE STRUCTURE

The Deliverable consists of the following sections:

Section 2: Explains the SHIELD framework and the way it contributes to WP2 objectives.

Section 3: Analysis and overview of the fundamental rights of individuals that might be affected by the operational usage of the INFINITY solution.

Section 4: Description of the applicable secondary data protection legislation for INFINITY covering the innovation phase (research and development) and the deployment phase (post-project operational usage).

Section 5: Specific considerations for the framework covering the use of AI, big data and ML.

Section 6: The general ethical framework and initial considerations on the societal impact.

Annex: Includes the questionnaire that was circulated within the consortium to provide an overview of national legislation.

2 SHIELD FRAMEWORK: SECURITY, HUMAN-CENTRED, INTEGRITY, ETHICAL, LEGAL AND DATA[3]

Due to the significance, scope and ambition of INFINITY to revolutionise contemporary multi-jurisdictional and data-driven investigations, a novel framework developed by CENTRIC will be applied to enhance the compliance of the project to the legal, ethical and data considerations outlined above. The SHIELD (Security, Human-centred[4], Integrity, Ethical, Legal and Data) Framework is designed specifically for research and development of advanced security solutions that utilise avant-garde technologies such as AI, big data and XR, amongst others[5].

As a result of the rapidly evolving technological landscape propelled by the so-called 'Law of Accelerating Returns'[6], there is often a time-lag between the pace of exponential change in technological advancement and legal regulations, and ethical standards to guide responsible innovation[7]. Several frameworks have been devised to offer dynamic approaches for guiding adherence to legal systems, ethical standards and societal values such as Values Sensitive Design[8], Networked System Ethics[9], Agile Ethics[10], Values at Play[11] and Worth-Centred Design[12], to name a few. However, as noted by Joh[13], the application of advanced and (semi-)automated big data analytics in LEA investigations complexifies the regulation of responsible development and use of these technologies due to considerations of accountability, transparency and acceptance by the public. Moreover, these approaches typically examine a narrow range of legal, ethical or societal aspects, leading to a lack of holistic approaches that encompass and integrate wide sets of relevant regulations, standards and values from design to development to implementation[14].

Taking these 'values in design' approaches as a launch pad while considering their limitations and seeking to address gaps, SHIELD has been developed to not only ensure compliance to legal regulations, ethical standards, and societal values, but also to advance them throughout the process of innovation and implementation. This section offers a summarisation of the SHIELD Framework core principles and levels of assessment as applied to the INFINITY Project, which are explained in the proceeding subsections and will be expanded upon as part of the social, legal and ethical impact assessment conducted in WP2.

[3] The SHIELD framework and the subsequent section was already explained in D1.4.
[4] Since the INFINITY Grant Agreement (883293), the principle of Health has evolved to Human-centred offer a more expansive and inclusive set of values for INFINITY.
[5] Reference to INFINITY Grant Agreement (883293), page 178.
[6] *Kurzweil, R*. (1999) The Age of Spiritual Machines: When Computers Exceed Human Intelligence. New York: Viking.
[7] *Brownsword, R., & Harel, A*. (2019). Law, liberty and technology: Criminal justice in the context of smart machines. International Journal of Law in Context, 15(2), 107-125.
[8] *Friedman, B., Kahn, P. H. Jr., Borning, A., & Huldtgren, A.* (2013). Value sensitive design and information systems. In N. Doorn, D. Schuurbiers & I. van de Poel, M. E. Gorman (Eds.), Early engagement and new technologies: Opening up the laboratory (pp. 55–95). Dordrecht: Springer.
[9] *Tamò-Larrieux, A*. (2018). Designing for Privacy and its Legal Framework Data Protection by Design and Default for the Internet of Things (First edition.) Cham: Springer International Publishing.
[10] *Kroener, I., Barnard-Wills, D., & Muraszkiewicz, J*. (2019). Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems. *Ethics and Information Technology*, 1–12.
[11] *M. Flanagan and H. Nissenbaum* (2014), Values at Play in Digital Games. Cambridge, MA: MIT Press.
[12] *Cockton, G.* (2006). Designing Worth is Worth Designing. Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles.
[13] *Joh EE* (2015) The new surveillance discretion: automated suspicion, big data, and policing. Research Paper No. 473, UC Davis Legal Studies Research Paper Series, December.
[14] *La Fors, et al*. (2019). Reassessing values for emerging big data technologies: integrating design-based and application-based approaches. Ethics and Information Technology, 21(3), 209–227.

2.1.1 CORE PRINCIPLES AND LEVELS OF ASSESSMENT

The SHIELD Framework is built on six core principles: Security, Human-centred, Integrity, Ethics, Legality and Data. These core principles provide a holistic framework that account for multifaceted considerations for the responsible innovation of advanced security technologies. In the context of INFINITY, these principles especially concerned with the use of AI, big data analytics and XR in LEA investigations of cybercrime, terrorism and hybrid threats. Each of these principles are applied at two Levels of Assessment that align with the project cycle and agile methodology of INFINITY: Innovation and Implementation. The application of these principles at the Innovation level will seek to ensure the highest standards of research and development are upheld, while implementation focusses on the practical application of solutions and their impact on the user and broader society. In line with the contention of La Fors *et al.*[15] that novel and dynamic legal, ethical and societal frameworks are required that keep pace with contemporary agile methodologies, Innovation and Implementation within the SHIELD Framework should not be considered as a sequential process, but rather as symbiotic parts of a whole that feedback into each other in reflection of the rapid and reiterated design, development and testing cycles of INFINITY.

Figure 2 SHIELD Framework

SHIELD	Innovation	Implementation
Security	Discretion, professional secrecy and confidentiality.	Security of the system from breach or tampering.
Human-centred	Uphold individual and collective societal values.	Ensuring human autonomy and discretion ('human-in-the-loop'); safeguarding the health and safety of the user.
Integrity	Responsible conduct in research to optimise confidence in findings.	Integrity of the system and of the user.
Legal	Compliance with GDPR and relevant codes governing research and development.	Compliance with LED and the specific governance, regulatory and legal frameworks of end users.
Ethical	Adherence to European Code of Conduct for Research Integrity and relevant academic ethical standards.	Algorithmic accountability and transparency; policing codes of ethics; mitigation of potential for misuse.
Data	Privacy and data protection by design and default.	Data minimisation and privacy enhancing technologies.

2.1.1.1 PRINCIPLE 1: SECURITY

During research and development, security is concerned with maintaining values of discretion, professional secrecy and confidentiality throughout project activities. It will ensure the correct management of EUCI (EU Classified Information), particularly LEA investigatory cases, tactics or procedures. It is critical to note that this does not equate to a lack of transparency in the project objectives and activities, but rather ensures that sensitive information is correctly handled which may otherwise jeopardise the safety and security of LEAs, society, Member States and the Union. Due to the high degree of sensitivity of the operational information INFINITY partners will access throughout the project, robust security protocols, including the use of appropriate encryption tools and procedures for the handling of EUCI, will be a crucial consideration for the project's research and the development of its technological solutions. At the implementation level, the

[15] *La Fors,* et al. (2019).

INFINITY system must be secure from breach, tampering or loss of information and evidence. This should be implemented through technological and organisational arrangements such as restricted and hierarchical access, secure servers and auditable controls with in-built protocols for management and sharing of information in cross-jurisdictional contexts.

2.1.1.2 PRINCIPLE 2: HUMAN-CENTRED

Human-centred values will also guide research and development in INFINITY. According to Zhang and Dong[16], this principle in research and development places humans at the centre of the innovation process and attempts a holistic understand needs through multi-disciplinary and user-centred research and development methodologies. The focus of all research and development activities and innovation outcomes will be on the human impact, both on the individual and collective societal level. As INFINITY is ultimately designed to protect and preserve EU societal values, its research will seek to promote societal values enshrined in the European Charter of Fundamental Rights. A key consideration that has significant implications for ensuring Human-centred implementation of INFINITY's solutions is determining the degree of agency to afford autonomous and semi-autonomous systems. Human-in-the-loop approaches consider the operator as 'system component' that maintains authority over (semi-) automated decision-making processes[17]. Measures such as these can improve human discretion in data-driven investigations utilising AI and ML capabilities. Health and wellbeing considerations for the use of INFINITY are also a key consideration, particularly the minimisation of the side effects of prolonged immersion in XR while retaining the cognitive benefits on performance and comprehension. This topic is addressed in D2.1 and D2.2.

2.1.1.3 PRINCIPLE 3: INTEGRITY

Integrity is key concept for research and development. It involves *responsible conduct of research*, defined as:

> 'Conducting research in ways that fulfil the professional responsibilities of researchers, as defined by their professional organizations, the institutions for which they work and, when relevant, the government and public'[18].

It also entails safeguarding against research misconduct, such as misrepresentation, inaccuracy and bias, by opting for methods and safeguards that optimise confidence in the veracity and reliability of findings. At the implementation level, integrity of the INFINITY system and its modular components entails the reliability of their performance, the accuracy and consistency of their outcomes, the system operating within its mandated operational and technical parameters and performs its intended functions unimpaired. Due to the data-driven nature of INFINITY's solutions, processes to ensure the integrity of data, such as error checking and validation measures, will play a key role to this end. INFINITY will also ensure that the integrity of the user is upheld so that at no point they will be compelled to undertake any action which they deem to be against their morality, conscience or beliefs.

2.1.1.4 PRINCIPLE 4: ETHICAL

[16] *Zhang T and Dong H* (2008) 'Human-centred design: an emergent conceptual model', Include2009, Royal College of Art, April 8-10, 2009, London Include2009 proceedings.
[17] *Steusloff, H. (*2016). Humans Are Back in the Loop! Would Production Process Related Ethics Support the Design, Operating, and Standardization of Safe, Secure, and Efficient Human-Machine Collaboration? *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 348–350, page 349.
[18] *Steneck, N.H.* (2006). Fostering integrity in research: Definitions, current knowledge, and future directions. *SCI ENG ETHICS* 12, 53–74, page 55.

INFINITY will adhere to the highest ethical standards throughout the research and development process. The project will be guided by the principles of The European Code of Conduct for Research Integrity foundational framework for research activities. This will include the selection of human participants and pilot scenarios to avoid potential biases. Additionally, these considerations will be extended to the development of AI to ensure its accountability and transparency. As implemented in policing, automated systems must be designed to offset potential algorithmic biases that may lead to potentially incorrect, unjustified or unfair results and ensure not only compliance with principles of legal fairness, but also moral and ethical considerations. Additionally, policing and criminal justice ethical standards should be consulted to ensure the alignment of INFINITY's solutions with codes of conduct. Moreover, the Consortium will undertake every possible measure to mitigate the potential for misuse of the research findings or technical outputs, which will be expounded in D11.5.

2.1.1.5 PRINCIPLE 5: LEGAL

A distinction is made within the project between research activities and real-life deployment of the solutions, as different legal foundations will apply to each area. During research and development, strict adherence to relevant legislations discussed in D1.4 governing the research activities carried out by INFINITY will be observed by the Consortium. The LED is the primary legal framework for the implementation of INFINITY's solutions by LEAs. INFINITY will also account for the end user's specific governance, regulatory and legal frameworks. The project will continually review these requirements in a real-life context throughout the project to facilitate compliance of the developed solutions in post-project deployment. Moreover, INFINITY will ensure the fundamental rights of EU citizens are lawfully upheld and advanced through its implementation.

2.1.1.6 PRINCIPLE 6: DATA

INFINITY will adhere to a strict data protection and privacy by design and default approach, discussed in depth in D1.4. From concept to deployment, data protection concerns will be at the forefront of considerations and form an integral part of development of the system. Where possible, privacy enhancing technology features will be incorporated into the final INFINITY system based on data minimisation principles, particularly those of necessity and proportionality utilised in policing, in order to address data protection and privacy concerns such as the overextension of surveillance powers.

3 FUNDAMENTAL RIGHTS AND PRIMARY LAW

Human rights are universally acknowledged rights that are inherent to all human beings. The EU is founded on these common values that are most prominently enshrined in the Charter of Fundamental Rights (hereinafter 'CFR'). These rights are to be protected during the course of any H2020 research project and should also be reflected in the output of such projects. Therefore, specific tasks in WP2 were designed during the Grant Agreement preparation to analyse, monitor and provide a legal framework for the INFINITY solution respecting these values. The subsequent paragraphs provide and analyse the relevant provisions of European human rights law.

Art 6 of the Treaty on European Union (hereinafter 'TEU') states the three formal sources of EU human rights law. The most relevant one in the EU is the Charter of Fundamental Rights of the European Union which was elevated to the level of EU primary law with the entry into force of the Treaty of Lisbon in 2009. In principle, the CFR can only be relied on within the framework of Union competences.[19] Furthermore, the Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms, also known as the European Convention on Human Rights (hereinafter 'ECHR'). Such accession shall not affect the Union's competences as defined in the Treaties. Which means that the Union has to act according to the principles set out in the ECHR, but no other Court (namely the European Court of Human Rights, hereinafter 'ECtHR') than the European Court of Justice (hereinafter 'CJEU') shall be competent to rule on Human Rights issues on EU level. ECHR infringements by member states can still be brought before the European Court of Human Rights, as the 27 Member States are party to the ECHR. Furthermore, the CFR was widely modelled on the ECHR, which is why it has a strong impact on EU fundamental rights law, even though the EU is not formally party to the ECHR. The third important source stated in Art 6(3) TEU are the general principles of EU law, which must and already have been developed from the national constitutions and human rights treaties binding to all the member states, especially the ECHR.[20] Those three sources of EU fundamental rights law are on the same level and can be applied cumulatively.[21]

For the purposes of this deliverable this analysis will focus on the fundamental rights which are most relevant for the execution of the INFINITY project. The following provisions of the CFR can be considered crucial for the project: Article 7 'Respect for private and family life' together with article 8 'Protection of personal data' are of pivotal importance and will be elaborated in more detail in section 3.1 and section 4. Specific characteristics of many AI technologies, including opacity ('black box-effect'), complexity, unpredictability and partially autonomous behaviour, may make it hard to verify compliance with, and may hamper the effective enforcement of rules existing in EU and national law that are meant to protect fundamental rights.[22] Therefore, further relevant fundamental rights provisions that might be of relevance are Article 20 of the CFR which enforces the right of equality before the law, and similarly, Article 21 of the Charter which stipulates the principles of non-discrimination. Article 47 'Fair trial'; Article 52 'Scope of guaranteed rights'; and Article 53 'Level of protection' are as well to be considered for this project. After a short overview of the mentioned fundamental rights, each of them, in particular Article 7 and 8 CFR, will be discussed in relation to the relevant secondary legislation. These laws (e.g. the GDPR) will act as the bases for the analysis of the legal issues and privacy impact assessments of each measure within the project.

[19] *Craig/de Búrca*, EU Law[6] (2015) 380, i.
[20] *Geiger* in *Geiger/Khan/Kotzur*, European Union Treaties Art 6 TEU Rz 34 (2015).
[21] *Geiger* in EU Treaties Art 6 TEU Rz 33.
[22] *EC*, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020).

Art 7 CFR guarantees that everyone's private and family life, home and communications must be respected. The aim of this fundamental right is therefore the protection of the individual's privacy from unlawful statutory interventions (in the case of the CFR from EU interventions). Art 7 CFR does not only encompass the prohibition of arbitrary sovereign interventions, but also positive obligations to ensure a certain level of privacy and protect individuals form third party interventions.[23] Art 7 CFR was modelled after Art 8 ECHR, therefore the interpretation of the latter provision can be relevant to the aforementioned.

According to Art 8(1) CFR '*everyone has the right to the protection of personal data concerning him or her*'. This fundamental right is closely related to Art 7 CFR and 8 ECHR, but the scope of protection of an individual's data pursuant to Art 8 CFR goes beyond, as not only data including information about one's private, family life and/or home is protected (private sphere). Today the right to data protection is especially realized through the GDPR, which will be discussed in detail in the next section.

A point of further note is that Articles 7 and 8 of the CFR are not absolute rights and may be limited under certain particular circumstances. Any interference with the protected rights is prohibited unless it falls within the limitations permitted by Article 52 of the CFR, which states the following:[24]

"*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*."

Art 47 CFR encompasses the right to an Effective Remedy and to a Fair Trial. These fundamental guarantees are not directly relevant to the project, but they should be kept in mind as the tools developed may be used in trials later on. For instance, the right to a fair hearing according to Art 47(2) CFR includes the right to a reasoned judgment.[25] If the decision is (partly) based on the outcome of an algorithm, developed within the project, it is important that the grounds for the automated decision are comprehensible. Therefore, it is important to develop understandable AI-algorithms. Furthermore, the judgement – and the basis for its decision – has to be fair and impartial, which is why unjustified or discriminatory biases in the algorithm (or the training data sets) could lead to an (indirect) infringement of this right.

In addition to fundamental rights, within the EU, primary law must also be taken into account in this context. As already mentioned, primary law commands the basis by which the EU is founded and by which new laws can be created. Pertinent for INFINTIY and D2.3 are both the Treaty on the Functioning of the European Union (hereinafter 'TFEU') and the TEU.

The TFEU confirms the basis of EU law, and in doing so it provides the scope of the EU's powers to legislate. This details the competencies of the EU while providing confirmation of the legal principles which need to be observed in the areas where EU law applies. The TFEU covers a broad range of fundamental principles and requirements for the functioning of the EU, and in particular Article 16(1) affirms that

1. *Everyone has the right to the protection of personal data concerning them*.

This provision corresponding with and reinforces the strength of Article 8 CFR. Further, Article 16(2) states that rules regarding the specificities of Article 16(1) must be laid down in EU law. As will be seen in the subsequent sections, the TFEU provides the basis by which the GDPR, the LED and their predecessor laws came into being.

[23] *Vested-Hansen* in *Peera/Hervey/Kenner*, The EU-Charter of fundamental rights (2014) Rz 07.18B.
[24] *Vested-Hansen* in The EU-Charter of fundamental rights, Art 7 Rz 07.06A.
[25] *Sayers* in The EU-Charter of fundamental rights Art 47 Rz 47.209.

The second principle document of primary legislation is the TEU which established the European Union under the Maastricht Treaty. It not only introduced the Euro and further unified the Member States, but relevant to this project, it confirms the application of Article 16 TFEU. Consequently, rules on privacy and data protection within the EU stem from fundamental rights and their essential place within EU law is confirmed in primary legislation.

3.1 DATA PROTECTION AS A FUNDAMENTAL RIGHT

Data protection and privacy are (among others; see above) fundamental human rights that need a special focus during the INFINITY research project. The right to protection of personal data is prominently enshrined in EU primary legislation such as Article 8 of the EU Charter of Fundamental Rights which is complemented by the right to privacy (Article 7 of the EUCFR). Article 8 of the EUCFR states that:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

Article 16 of the Treaty on the Functioning of the European Union (TFEU), reinforces the fundamental necessity of data protection:

> *1. Everyone has the right to the protection of personal data concerning them.*

The right to respect for private and family life as contained in Article 8 of the European Convention on Human Rights also covers aspects of data protection. However, these rights may be subject to limitations under Article 52(1) of the Charter which defines the scope of the guaranteed rights and holds that any limitation to the exercise of rights and freedoms recognised by the EU Charter must be provided for by law and respect the essence of these rights and freedoms. Moreover, such limitations may only be made subject to the principles of necessity and proportionality. Based on the core values of EU primary law there is a number of relevant secondary legislation in the domain of data protection that is applicable for research activities within INFINITY as well as deployment post-project in an operational context. This brief analysis of fundamental rights and primary law act as the foundation for the following look into the relevant secondary legislation within the EU.

4 DATA PROTECTION FRAMEWORK - SECONDARY LEGISLATION

While Data Protection is a fundamental right in primary legislation, there is an extensive body of secondary legislation that upholds this fundamental right. This section will begin with a brief introduction of all legislative acts covering secondary data protection legislation and national data protection acts that may be of relevance for the INFINITY project. D1.4 has already provided guidance for data processing under the GDPR[26] within the research context. The specific nature of judicial cooperation in criminal matters and police cooperation necessitates specific data protection rules in these fields, as also acknowledged in Declaration No 21 annexed to the TEU and TFEU. The framework applicable for the post-project use, namely Directive 2016/680[27] (hereinafter the LED) and the Europol Regulation,[28] is therefore distinct from the GDPR and will be added within this document. Special attention will be paid to the delineation of these distinct yet interconnected frameworks. It must be understood that the EU data protection legal framework has developed to recognise '***two distinct regimes of data protection*** *that could potentially apply to information sharing […] one general and one for data processing by law enforcement authorities for law enforcement purposes*'.[29] The following paragraphs will first outline the distinct legislation, namely the GDPR, the LED, the ER and their distinctive nature as well as the relevant national legislations. As the European legislator ensured that both the LED and the GDPR, though distinct in their application, firmly maintain a level of consistency in the same terminology and principles of data protection, we will subsequently give an overview of the relevant terminology, principles and data subject rights attached to the data protection framework for both processing purposes. This analysis of the relevant legal sources will contribute to fulfilling the aim of supporting the partners in overlooking and identifying their obligations when personal data is envisaged to be processed. A risk analysis and compliance of INFINITY, both during and post-project, with this framework will be further elaborated in subsequent deliverables.

4.1 GDPR

The EU General Data Protection Regulation (GDPR) entered into force on the 25th May 2018 throughout the European Union and lays down rules relating to the protection of natural persons with regard to the processing of their personal data. As an EU Regulation, the GDPR is a binding legislative instrument, thus requiring no national legal transposition, like for example the LED, and applying in a harmonized manner across all EU Member States. There are however a number of so called 'opening clauses' and derogations in which Member States Law may differ in the application of the GDPR (see below and consult D1.4), because Member States are allowed to modify the provision and to introduce a more permissive or restrictive implementation. Specifically, in the context of INFINITY the GDPR may be applicable to the activities **for research purposes. D1.4** constitutes the first point of reference for data processing in research settings. For the sake of completeness and comprehensibility, GDPR considerations are also elaborated within this document und the relevant provisions are further analysed.

[26] 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).
[27] 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.
[28] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.
[29] *Nadezhda Purtova*, 'Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships ' [2018] 8(1) International Data Privacy Law 52-68.

4.2 LED 2016/680

The Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data that also apply to judicial cooperation in criminal matters and police cooperation. This process led to the adoption of the so-called LED. The GDPR and the Law Enforcement Directive 2016/680 (LED) have a distinct scope and a mutually exclusive application. The LED provides the EU legal basis for personal data processing and exchange in a criminal **law enforcement context**. The LED lays down the rules relating to 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, including the safeguarding against and the prevention of threats to public security.*[30]

The primary distinction between the application of either the GDPR or LED is the purpose for processing. In accordance with the purposes of processing set out in Article 1(1) of the LED, the LED does not apply to the processing of personal data within the research and development phases of the INFINITY project. The purposes of processing during the course of the project are for scientific research purposes and not for the abovementioned law enforcement purposes. If the purposes for processing correspond to those mentioned above from Article 1(1) LED, then the LED applies and the GDPR does not, which will be the situation for the real-life deployment of the solution. Within the INFINITY project, LEAs should pay close attention to the distinct applications between the LED and the GDPR, and when in doubt consult the list provided in Article 1(1) of the LED.

The LED provides requirements which set out the minimum level of harmonisation and the following results to be achieved by the Member State. Being a Directive however allows Member States to have a level of discretion on how exactly they want to implement the Directive into national law (see below). A Member State may therefore provide higher standards than the ones initially set out in the Directive. However, it should be noted that in accordance with the purposes of the LED, it provides significantly more limitations on the rights of the data subject than the GDPR. This difference makes legislative sense given the sensitive nature of the fight against crime and will be discussed in more detail in subsequent sections. LEAs will have to apply the GDPR for activities applicable within the research context.

4.3 EUROPOL REGULATION

Additionally, it needs to be considered that for Europol as an EU Agency neither the GDPR[31] nor the LED does apply. Nevertheless, the agency claims to have one of the strongest data protection regimes in the world, offering higher standards than those found in the majority of Member States. The legal framework for data processing activities by Europol was established in 2016, namely the Europol Regulation.[32] The ER has autonomous data protection rules set out that are consistent with other relevant data protection instruments in the area of police cooperation such as the LED. Notably, the ER established a so-called Europol Cooperation Board composed of the EDPS and the national DPAs,[33] which provides the agency with an exemplary external oversight mechanism. Processing activities of Europol inherit a special position regarding data processing activities both, within and after the project, that must be born in mind.

[30] LED, Article 1(1).
[31] GDPR, Article 2(3).
[32] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.
[33] Europol Regulation, Article 43.

The EC has recently issued a proposal for the amendment of the ER which foresees the full applicability of the EU-DPR for Europol. Amongst others the proposal introduces a new provision on the processing of personal data for research and innovation to take due account of the stronger role Europol will play in these areas and the impact thereof on the processing of personal data and provide for additional safeguards.[34] The proposal is now in the stage of the legislative procedure and the outcome is this process cannot be anticipated. However, the new applicable legislation can be expected to come into force in the future and will certainly impact at least the deployment phase of the project.

For the time being the decisive criterion for the applicable data protection framework is whether 'operational personal data' or 'non-operational personal data' in terms of the EU-DPR is processed. Article 3(3) of the EU-DPR defines it as the following:

operational personal data means all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies.

When it comes to non-operational matters within INFINITY research environment, Europol applies Regulation 2018/1725[35]. Regarding the real-life deployment of the solution by Europol the Europol Regulation (ER) is applicable. All these legal frameworks build on the same data protection principles that will be duly observed in the execution of the project and are provided for in this document to facilitate compliance.

4.4 NATIONAL DATA PROTECTION LAWS

As already briefly discussed in the previous sections, an EU Regulation, such as the GDPR is a legal act which is directly applicable to an EU Member State and therefore applies uniformly throughout the EU from the moment it enters into force. As such, Regulations are absolutely binding on all EU countries. Directives on the other hand, require EU Member States to transpose the legal measures into national law. Consequently, the discretion of each Member State to implement Directives means that there are differences in the national application of the laws throughout each EU country.

4.4.1 TRANSPOSITION OF THE LED

Directives require EU Member States to transpose the legal measures into their national law. Consequently, the discretion of each Member State to implement Directives means that there are differences in the national application of the laws throughout each EU country. Specifically, the LED, as other EU Directives stipulates the requirements of national transposition. Ultimately, in accordance with Article 63 of the Directive, when Member States adopt the provisions contained in the Directive, they must refer to the Directive within their national law. Each national law implementing the Directive can be found in an online directory.[36] For the

[34] Proposal for a regulation of the European parliament and of the council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/09122020_commission_proposal_regulation_european_parliament_council_european_agency_law_enforcement_cooperation_replacing_regulation_2016-794_po-2020-8998_com-2020_796_en.pdf (accessed 11.02.2020) page 14.

[35] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/936/JHA and 2009/968/JHA.

[36] Document 32016L0680: National transposition measures communicated by the Member States concerning: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of

purpose of the project, we have additionally circulated a questionnaire that should help identify and complement the national legislations that are applicable. In terms of practical reference within the project, the law connected to the corresponding country where an activity is being carried out, or with whom data is being exchanged should be sought.

The grounds for processing must be provided for in data protection legislation, whether in Union or Member State law, through the transposition of Directive 2016/680. A point to note is that as with the GDPR,[37] the LED provides data protection framework and then the national legal provisions which substantiate the legal basis for processing. An example of this in the national law of the transposition of the LED in Austria is the Data Protection Act §§ 36ff and the legal powers of the police to process the data are substantiated in the Security Police Act §§ 52ff. With reference to this, there is a differentiation between national transposition of the LED and the national law which substantiates the legal basis for processing by LEAs – these instances may feature overlaps depending on the national jurisdiction, but for some jurisdictions the two are connected and yet distinct.

4.4.2 OPENING CLAUSES GDPR

In addition to the variances between national law and the Directive, there may be some variation between Member States on regarding the application of the GDPR. The GDPR does provide what are known as "Opening Clauses". Opening Clauses are provisions which provide scope for EU Member States to enact their own specific national measures relating to data protection. These opening clauses, such as provided for in Article 9, 23 or 89 of the GDPR for example, allow Member States to modify the provision and to introduce a more permissive or restrictive implementation (depending on the opening clause). The use of opening clauses is always optional and may vary from Member State to Member State and must be borne in mind for the course of the project.

Derogations provide Member States with a certain degree of flexibility in deciding how particular provisions will apply. Article 89, which relates to data processing activities for research purposes, might be of particular relevance for the INFINITY project and the activities of LEAs. Article 89(2) states the following:

> *Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.*

The GDPR does not exactly define what qualifies as scientific research. Recital 159 GDPR suggests a broad understanding of the term "scientific research", encompassing also e.g. privately funded research. The term may not be stretched beyond its common meaning though. The former Article 29 Working Party understands that 'scientific research' in this context means '*a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice*'.[38]

---

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 (EUR-Lex), https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0680 (accessed 09.11.2020).

[37] Specifically, Article 6(1)(c) GDPR.

[38] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 (as last revised and adopted on 10 April 2018), page 28.

Consequently, for the purposes of research certain rights of the data subject (see section 4.8), such as the right of access to data by the data subject (Article 15), the right to rectification (Article 16), the right to restriction of processing (Article 18), and the right to object (Article 21) may all be limited, provided those special derogations are foreseen in national law. Additionally, any limitations must however be subject to appropriate safeguards in accordance with the GDPR and the fundamental rights and freedoms of the data subject. Examples of such safeguards include the employment of technical and organisational measures to ensure the respect for the principle of data minimisation, and the pseudonymisation of the data subject as long as the purposes for the limitation can still be fulfilled. The overall use of Article 89 within the context of the INFINITY project will be evaluated depending on the specificities, circumstances and data sources for the pilot demonstrations. In any case, following the ECs Ethics Review, the beneficiaries, in accordance with their DPOs, will check if special derogations pertaining to the rights of data subjects have been established under the national legislation of the country where the research takes place and submit a declaration, that they will comply with the respective legislation if they are in the scope of its application by specific research activities.[39]

4.4.3 LEGISLATIVE OVERSIGHT OF RELEVANT NATIONAL DATA PROTECTION LEGISLATION AND OPENING CLAUSES

For the execution of T2.3 it was considered necessary to issue a partner questionnaire and aid in the objective to provide the widest and most detailed analysis of the relevant legal, societal and ethical framework possible, especially by also including national legislation. The objective was the collect, analyse and display the differences in the national legal frameworks with regard to the relevant opening clauses of the GDPR and the national transpositions of the LED.

The following tables provide the specific legal application of the GDPR and LED based on each Member State provided. The tables feature interpretations and translations of national law gathered from partners, their DPOs and legal departments, as a result of the D2.3 questionnaire attached to this report. The aim of these tables is to provide the project with the necessary legislative oversight of the national law differences within the EU and the relevant third countries.

National Transposition of the LED			
Country	National law	Summary of content	Relevant Partner(s)
Belgium	Belgische Kaderwet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens van 30 juli 2018 en meer bepaald Titel 2 Wet op het Politieambt, artikel 44	National Transposition of Directive 2016/680: Belgian framework legislation of 30 July 2018 concerning the protection of natural persons with regard to the processing of personal data and more specifically Title 2 (Belgische Kaderwet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens van 30 juli 2018 en meer bepaald Titel 2) Law on the Police Profession, article 44 and following (Wet op het Politieambt, artikel 44 en volgenden)	POLITIEZONE VAN ANTWERPEN (PZA)
		Competent authority: Those departments that are exclusively or primarily responsible for the investigation and detection of criminal offenses:	

[39] D11.3 is the point of reference.

		• police forces; • the judicial authorities; • the Investigation Services of the Standing Committee P and of the Standing Committee I; • the General Inspection Services of the Federal Police (AIG); • the Passenger Information Unit (PIE) under the PNR legislation; • the Financial Information Processing Unit (CFI); • the General Administration of Customs and Excise	
Portugal	Portuguese Law No. 59/2019	Transposes Directive 2016/680 into National law; approves rules on processing of personal data for purposes of prevention, detection, investigation or prosecution of criminal offenses. Definition of competent authority "refers to any person or organization that has the legally delegated or invested authority, capacity, or power to perform a designated function. . Similarly, once an authority is delegated to perform a certain act, only the competent authority is entitled to take accounts therefrom and no one else. In security domain, competent authority is a public authority responsible for the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of criminal sanctions, including the safeguarding and prevention of threats to public security." Article 5 – personal data processing lawful if required by law and to the extent necessary for exercise of assigning competent authority. Article 6 – for special categories of data, processing okay only if strictly necessary and subject to adequate safeguards to protect rights and freedoms of data subject and if it is: (a) authorized by law; (b) intended to protect the vital interests of the data subject or of another individual; or (c) is related to data manifestly made public by the data subject. Profile definitions that lead to discrimination against natural persons based on the special categories of personal data prohibited. Article 7 – further processing okay if purpose is one of those enumerated in Art. 1 and: (1) controller authorized by law to process data for that purpose and (b) processing necessary and proportionate to the other purpose under the law. This includes further processing for public interest and for research/statistical purposes. Article 12 – deadlines for conservation and evaluation – processing can be done only during period necessary for pursuit of the purposes of the collection or of the subsequent processing authorized under article 7.	Ministério da Justiça (PJ)
	Portuguese Law No. 37/2015 – Criminal Identification	Criminal record effects recorded information on fingerprints to be kept for 10 years after conviction	

	Portuguese Decree-Law No. 352/99 - PJ Database	Information kept for the purposes of prevention and criminal investigation to be kept for max of 30 years.	
	Portuguese Law No. 5/2008 – DNA profile database	DNA profiles and corresponding personal data to be kept for length of convict's sentence plus a max of 10 years or up to 23 years in case of convictions for crimes against freedom and sexual self determination.	
	Portuguese Laws providing "legal basis" per Directive 2016/680	• Decree Law nº137 / 2019, 13 September 13 - Polícia Judiciária Organic Law; • Law no. 49/2008, August 27 - Law on the organization of Criminal Investigation; • Law no. 23/2008, August 29 - Internal Security Law; • Decree-Law no. 48/1995, March 15 - Penal Code Constitution of the Portuguese Republic Constitution (Article 35- Use of information technology); • Law no. 41/2004, of 18 August - PROTECTION OF PERSONAL DATA AND PRIVACY IN TELECOMMUNICATIONS; • Law No. 43/2004, of 18 August - Organization and functioning of the National Data Protection Commission; • Law no. 58/2019, of 8 August; • Law no. 59/2019, of 8 August; • Polícia Judiciária Organic Law – Decree Law nº137/2019, of 13 September; • Polícia Judiciária Database Regulation – Decree Law nº352/99, of 3 September; • Cybercrime Law – Law 109/2009, 15 of september; https://www.anacom.pt/render.jsp?contentId=985560	
Greece	Greek Law 4624/2019 (FEK A'137 29—08- 2019)	Transposes Directive 2016/680 into national Greek Law; no official translation yet. Does not include definition for "competent authority"	HELLENIC POLICE (HP); CERTH; KEMEA
	Greek Law 4624/2019 (FEK A'137 29—08- 2019)	Competent Authority: Article 44 par.1 of L.4624/2019 which implements article 3 of the Directive 2016/680, does not include a specific definition of the term "competent authority". Also , according to article 4 of L.4624/2019, in general a) "public body": public authorities, independent and regulatory administrative authorities, legal persons governed by public law, first and second-level local government authorities with their legal persons and their legal entities, state-owned or public undertakings and	

		agencies, legal persons governed by private law which are state-owned or regularly receive at least 50% of their annual budget in the form of state subsidies, or their administration is designated by the state. b) "private body": any natural or legal person or group of persons without legal personality which does not fall within the definition of the above. Also, according to article 43 of L.4624/2019, which implements articles 1 and 2 of the Directive states: The provisions of this Chapter shall apply to the processing of personal data by public authorities which are competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In the above cases, the public authorities are always considered as controllers. Where, in this Chapter, provisions for processors are included, its provisions shall also apply to them. From the above, it is considered that authority responsible is HELLENIC POLICE.	
	Greek Law 4624/2019 (FEK A'137 29—08- 2019)	Legal basis for processing of personal data: Article 8 of Directive 2016/680 which stipulates the relevant quotation, has not been transported into Hellenic Law, therefore the respective national laws have not been clarified.[40] presidential decree 178/2014 (edited by presidential decree 93/2020) Article 5 law 4624/2019 Legal basis for the processing of personal data by public bodies Public bodies may process personal data where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority conferred on the controller. presidential decree 135/2013 article 3 The competent law enforcement authorities may, upon request, exchange information and data during the investigation of the crime or during the operation of collecting information and data related to this crime. article 7 law enforcement authorities shall provide information and data to the law enforcement authorities of other Member States concerned, without prior request, if it is considered on objective grounds that such information and data could facilitate the detection, prevention or investigation of criminal offenses contained in case e ' of article 2. (Crimes are considered the following : aa) criminal organization, bb) terrorist acts, cc) trafficking in human beings and	

[40] <https://www.dpa.gr/sites/default/files/2020-01/gnomodotisi%201_2020.pdf> (24.02.2021).

		trafficking in human beings, dd) infringements on sexual freedom and exploitation of the sexual life of minors, child pornography, ee) trafficking in human beings; ff) illicit trafficking in arms, ammunition and explosives, gg) crimes of corruption and bribery, hh) crimes against the economic interests of the European Communities (Law 2803/2000, A'48), ii) money laundering criminal activities, ii) currency crimes including the euro, jaa) computer crimes, lb) environmental crimes, including illicit trade in endangered species and illicit trade in endangered plant species and plant species; assistance for illegal entry and residence in the country, n.d) Intentional homicide, grievous bodily harm, n trafficking in human organs and tissues, abduction, unlawful detention, abduction and hostage-taking, qc) racism and xenophobia, (iii) organized or armed robbery and theft, fraud, extortion, extortion, counterfeiting and piracy of goods, kg) forgery of public documents and trafficking in counterfeit documents, trafficking in stolen vehicles, burglary, rape, , arson, etc. crimes within the jurisdiction of the International Criminal Court, lala) hijacking and piracy, etc.) sabotage.) The spontaneous exchange is carried out in accordance with the provisions of Greek legislation.	
	Greek Law 4624/2019, Article 30	Makes use of GDPR Art. 9 derogation and permits processing w/o consent when it is “necessary for scientific or historical research purposes or the collection and retention of statistics and [] controller’s interest overrides data subject’s…” and so long as controller exercises measures to protect data subject’s interests. Derogation to GDPR Arts. 15, 16, 18, and 21 if data subject rights are likely to impede fulfilment of the above, data subject rights restricted. Under Art. 15 – right to access does not apply where data necessary for scientific purposes and providing information requires disproportionate effort. Data subjects can be named in publication if consent or if necessary for the presentation of research results (if latter case, must pseudonymize).	
Germany	„Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 / DSGVO und zur Umsetzung der Richtlinie (EU) 2016/680 / JI-Richtlinie (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU)“	National Transposition of Directive 2016/680: Translation: “Act to adapt data protection law to Regulation (EU) 2016/679 and to implement Directive (EU) 2016/680 (Data Protection Adaptation and Implementation Act EU - DSAnpUG-EU “	Hochschule für den öffentlichen Dienst in Bayern (BHFOD)
		Competent authority: No direct definition of "competent authorities". The law applies to (1) public authorities of the federal government	

		(2) public authorities of the federal states, insofar as data protection is not regulated by state law and insofar as they (a) implement federal law or (b) act as organs of the administration of justice and are not involved Administrative units. Regarding (1) Federal public bodies are the authorities, the administration of justice and other federal institutions organized under public law, the federal corporations, the institutions and foundations under public law and their associations regardless of their legal form. Regarding (2) Public authorities of the federal states are the authorities, the organs of the administration of justice and other bodies organized under public law of a federal state, a municipality, a municipal association or other legal entities under public law and their associations regardless of the legal form.	
	Federal Criminal Police Office Act - BKAG Federal Police Act – BPolG Criminal Procedure Code - StPO Police laws of the federal states	Legal basis for processing of personal data pursuant to Directive 2016/680: Law on the Federal Criminal Police Office and cooperation between the Federation and the Federal States in criminal police matters (Federal Criminal Police Office Act - BKAG Law on the Federal Police (Federal Police Act – BPGol) Criminal Procedure Code (Strafprozessordnung, StPO) Police laws of the federal states: e.g. Law on the Tasks and Powers of the Bavarian State Police (Police Tasks Act – PAG)	
	Telecommunications Act (TKG) in conjunction with the Criminal Procedure Code (StPO)	National regulations on retention of data or bulk data collection (for law enforcement or scientific research purposes).	
North Ireland (UK)	Data Protection Act 2018 The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019[41]	National Transposition of Directive 2016/680: Transposes the LED into national law. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 is relevant because of Brexit. More details see section 4.5.1 of this Deliverable.	Police Services of Northern Ireland (PSNI)
	Data Protection Act 2018, Part 3, art 30 and schedule	Competent Authority: Defined in Data Protection Act 2018, Part 3, art 30 and	

[41] <http://www.legislation.gov.uk/uksi/2019/419/contents/made> (26.02.2021).

	including	schedule 7 including: • Information Commissioner's Office • PSNI- Chief Constable • N.I. Government departments • Chief Officer of Harbour Police • The Police Ombudsman for Northern Ireland • The Director General of the National Crime Agency • The Director of the Serious Fraud Office • The Financial Conduct Authority • The Criminal Cases Review Commission • The Parole Commissioners for N.I • The Probation Board for N.I • The Director of Public Prosecutions for N.I	
	Police Act (NI) 2000 Data Protection Act, (DPA) 2018 Part 3 and 4	Legal basis for processing of personal data pursuant to Directive 2016/680: Police Act (NI) 2000 defines the functions of the law enforcement agency and lawful basis for processing are mainly but not limited to: Law Enforcement processing: Data Protection Act, (DPA) 2018 Part 3 Intelligence Processing: (DPA Part 4)	

Opening Clauses Art. 89 GDPR			
Country	National law	Summary of content	Relevant Partner(s)
Belgium	Title 4 (art 186-208) of the Belgian framework legislation of 30 July 2018 concerning the processing for archiving in the public interest, scientific or historical research or statistical purposes referred to in Article 89 §§ 2 and 3 of the Regulation	Makes use of GDPR Art. 89 opening clause on processing of personal data for archiving purposes in the public interest	POLITIEZONE VAN ANTWERPEN (PZA)
	Law on the Police Profession	National regulations on retention of data or bulk data collection: Law on the Police Profession, Article 44 and following (Wet op het Politieambt, artikel 44 en volgenden) Ministerial circular PLP 40 concerning the archives of the Local Police: Records selection list and retention periods (9 February 2006)	
Germany	Art. 27, 50 Federal Data Protection Act	National implementation of opening clause regarding the processing of personal data for scientific research	Hochschule für den

	(BDSG); Art. 21 Federal Criminal Police Office Act (BKAG); Art. 25 Bavarian Data Protection Act (BayDSG); Art. 54 Police Tasks Act (PAG)	purposes.	öffentlichen Dienst in Bayern (BHFOD)
Greece	Greek Law 4624/2019, Article 30	Makes use of GDPR Art. 9 derogation and permits processing w/o consent when it is "necessary for scientific or historical research purposes or the collection and retention of statistics and [] controller's interest overrides data subject's…" and so long as controller exercises measures to protect data subject's interests. Derogation to GDPR Arts. 15, 16, 18, and 21 if data subject rights are likely to impede fulfilment of the above, data subject rights restricted. Under Art. 15 – right to access does not apply where data necessary for scientific purposes and providing information requires disproportionate effort. Data subjects can be named in publication if consent or if necessary for the presentation of research results (if latter case, must pseudonymize).	HELLENIC POLICE (HP); CERTH; KEMEA
	Greek Law 4624/2019, Art. 29	Makes use of GDPR Art. 89 opening clause on processing of personal data for archiving purposes in the public interest.	
	Greek Law 4624/2019, Art. 73	Data storage for law enforcement purposes: Where Directive 2016/680 applies, Greek law states the controller "shall provide for data erasure or periodic review of the need for the storage…."	
	Greek Law 4624/2019, Art. 45, paragraph 1(d)	Storage for scientific purposes, principle of "storage limitation" applies and for inaccuracies "without delay erasure or rectification of inaccurate personal data, having regard to the purposes for which they are processed".	
Italy	Italian Data Protection Code	The articles from the Italian Data Protection Code, relevant for INFINITY could be Art. 105 and especially Art. 110-a. Art. 105: 1. No personal data that is processed for statistical purposes or scientific research purposes may be used for taking decisions or measures with regard to the data subject or else with a view to processing data for different purposes. 2. Statistical or scientific research purposes shall have to be specified unambiguously and made known to the data subject in accordance with Articles 13 and 14 of the Regulation as also related to Section 106(2), letter b), of this Code and Section 6-a of legislative decree No 322 of 06.09.89 as subsequently amended. 3. Where specific circumstances referred to in the rules of conduct as per Section 106 are such as to allow an entity to respond in the name and on behalf of another entity, being a family member of or co-habiting with the latter,	INGENGERIA INFORMATIC SPA (ENG)

		the data subject may also be informed by the agency of the respondent. 4. As for processing operations for statistical purposes or scientific research purposes concerning data collected for other purposes, no information shall have to be provided to data subjects if it entails a disproportionate effort compared with the right to be protected – on condition that those operations have been appropriately publicized as laid down in the rules of conduct referred to in Section 106. 110-a (Further processing of personal data by third parties for scientific research or statistical purposes): 1. The Garante may authorise further processing of personal data, including the special categories of personal data referred to in Article 9 of the Regulation, for scientific research purposes or statistical purposes by third parties that carry out such activities to a prevailing extent if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes. In such cases, the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects in accordance with Article 89 of the Regulation including arrangements for the prior minimization and anonymization of the data.	
	Art 99(1) Italian Data Protection Code	Under the Italian Data Protection Code, in Art.99(1) it is stated the following: "The processing of personal data for storage in the public interest, for scientific or historical research or for statistical purposes may be carried out beyond the retention period necessary to achieve the various purposes for which the data were previously collected or processed."	
Portugal	Portuguese Law No. 58/2019	Article 31–provides procedures for treatment of data when processed for purposes of public interest archiving, scientific research or historical purposes – data minimization, anonymization, and pseudonymization where possible.	Ministério da Justiça (PJ)
Spain	2/2018 Organic Law, of Personal Data Protection and Digital Rights Guarantee	With regards to Article 89, the Spanish transposition of the GDPR (2/2018 Organic Law, of Personal Data Protection and Digital Rights Guarantee) only foresees data processing for health research purposes, particularly for biomedical purposes in its 17th additional provision.	VICOM, UPM
	Article 28, 2/2018 Organic Law, of Personal Data Protection and Digital Rights Guarantee	According to the Spanish 2/2018 Organic Law, article 28 specifies that GDPR articles 24 and 25 will be born in mind when determining technical and organisational measures to guarantee that data processing is done in compliance with all regulations. Also, it states that in order to adopt the necessary measures, it will be taken into account that massive data treatment (art. 28.2.a) may involve major risks.	

4.5 DATA TRANSFERS TO NON-EU COUNTRIES

As the INFINITY project involves a partner from the United States, two from the UK and another one is pending to be added from Switzerland, the GDPR rules regarding transfers of personal data to third countries or international organisations[42] might be of relevance to the project. Chapter V and more specifically article 45 of the GDPR provides the rules in which data transfers to third countries may be made on the basis of an 'adequacy decision'. An adequacy decision determines whether a country outside of the EU has an adequate level of data protection in accordance with the GDPR. An adequacy agreement takes into account the entire legal and political context of the country in question into account, considerations include but are not restricted to the rule of law, respect for human rights and fundamental freedoms and relevant legislation.[43] Additionally, in making the adequacy decision both the presence of an effective independent supervisory authority is considered, as is the notion of whether and which international agreements the country has entered into. Currently, the European Commission has recognised Switzerland along a number of other third countries as providing adequate data protection levels.[44] In terms of practicalities and data exchange, this means that in accordance with Article 45(1) GDPR, any data transfer between Switzerland and EEA Member States will not require any specific authorisation as the adequacy level of their data protection legislation and practices have already been confirmed.

For the purposes of data transfers in real-life scenarios of LEAs, Article 36 lays down the conditions for transfers on the basis of an adequacy decision. The requirements detailed in Article 36 of the LED are the same as those given in Article 45 of the GDPR.

Data transfers to third countries which lack an adequacy agreement are certainly possible, but the process is subject to many conditions which must be confirmed prior to any data transfers. One possible solution that might be the most appropriate for the INFINITY project is the adoption of standard data protection clauses (hereinafter 'SCC') as mentioned in Article 46(1)(c) of the GDPR.

4.5.1 UNITED KINGDOM

The UK left the EU on 31 January 2020 and entered into a transition period, which ended on 31 December 2020. In principle, the GDPR ceased to apply for the UK and the UK is now considered a third country in relation to the EU in terms of the GDPR. However, the EU and the UK have reached an agreement (the so-called 'Trade Agreement'[45]) which introduces a so-called 'bridging mechanism' that allows personal data flows to continue for the time being. The agreement specifies a period of four months which can be extended up to six months.

For transfers from the EEA into the UK, the EU GDPR rules on restricted transfers (GDPR, Chapter V as mentioned above) will apply. The UK Government is seeking a European Commission 'adequacy decision' which will allow the free flow of data under those rules. The EU has agreed to delay transfer restrictions for at least four months (up to six months) to allow time for the EU to consider whether to grant such an 'adequacy decision', as part of the new trade deal. In the absence of an EU 'adequacy decision' at the end of the bridge, these transfers will need to comply with EU GDPR transfer rules. It remains to be seen whether the European Commission will put an adequacy decision in place during that time period. Just recently on the 19th of February 2021 the EC announced that they have launched the procedure for the adoption of two adequacy

[42] GDPR, Article 44ff.
[43] GDPR, Article 45 (2) (a).
[44] European Commission, adequacy decisions https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 10.02.2020).
[45] https://ec.europa.eu/info/sites/info/files/draft_eu-uk_trade_and_cooperation_agreement.pdf

decisions for transfers of personal data to the United Kingdom, under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) respectively.[46]

Restricted transfers from the UK to other countries, including to the EEA, are now subject to transfer rules under the UK regime. These UK transfer rules broadly mirror the EU GDPR rules, but the UK has the independence to keep the framework under review. The UK government has the power to make its own 'adequacy decisions' in relation to third countries and international organisations. In the UK regime these are now known as 'adequacy regulations'. The UK has deemed the EEA to be adequate on a transitional basis. That means that a free flow of data from the UK to the EEA can continue for a few years (likely to last until December 2024) by which time the UK will have conducted formal adequacy assessments of the EEA.[47]

4.5.2 UNITED STATES

EU-US data transfers have been an ongoing issue for an extensive period of time and will continue to do so in the future. In its recent judgment *Schrems II*[48] the CJEU invalidated the adequacy decision that existed between the EU and the U.S. In the absence of an adequacy decision, we again need to rely on one of the transfer tools listed under Articles 46 GDPR for transfers that are regular and repetitive (SCCs are considered to be the most appropriate option for the project). The CJEU reemphasised, that the protection granted to personal data under the GDPR must travel with the data when personal data is transferred to non-EU countries. The Court additionally stated that controllers and processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. In those cases, the Court still leaves open the possibility for exporters to implement supplementary measures (such as for example encryption) that fill these gaps in the protection and bring it up to the level required by EU law.[49]

4.6 TERMINOLOGY

As there are many similarities and overlaps between the content of the GDPR, the LED, the EU-DPR and the ER (especially in terms of data protection terminology), the terminology and principles will be elaborated together. However, the following subsections will, where necessary distinguish between any differences or variations between the different pieces of legislation (with special focus on the GDPR and the LED).

4.6.1 PROCESSING OF PERSONAL DATA

The EU data protection legislation (GDPR as well as the LED) applies only to the *processing* of *personal* data. Since the EU data protection legislation only deals with the processing of personal data, the distinction of personal and non-personal data (also called anonymous data) is crucial for all activities of the project. Article 4 (1) defines personal data as

[46] The press release of the EC and the drafts are available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_en (accessed 19.02.2021).
[47] https://www.fieldfisher.com/en/insights/an-adequate-agreement-what-the-brexit-deal-means-f#_ftn25
[48] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, (hereinafter C-311/18 *Schrems II*), second finding.
[49] EDPB recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (adopted on 10.11.2020), to be found here: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (accessed 11.01.2021).

> ***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.*

The Court of Justice has clarified while determining whether someone is identifiable or not, an 'objective' and 'relative' criterion must be employed. Namely, the test is objective if the personal data concerned is identifiable personal data in the hands of anyone and they can link the information to the person. The test is relative when it would only be personal data in the hands of a party who has additional lawful means of accessing connecting information which would identify the individual.[50]

Another principle term contained in both pieces of data protection legislation concerns the variety of activities which can constitute data 'processing'. Conveniently, both the GPDR and the LED refer to the same list of processing methods. As such:

> ***'processing'*** *means 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;*[51]

Consequently, if a party has and does anything with personal data within the EU as set out in this list then they are processing personal data and are either subject to the requirements of the GDPR, the LED, the Europol Regulation or the EU-DPR depending upon processor and the purposes of the processing.

The use of fully anonymized, synthetic, dummy, fake or any other data that does not qualify as personal data, significantly minimises the duties and potential liabilities of all partners engaging in processing activities. Most importantly it minimises any possible risks to the rights and freedoms of data subjects. Therefore, the use of non-personal data is strongly advised whenever this is possible and considered functional for the purposes of the processing.

4.6.1.1 PSEUDONYMISATION AND ANONYMISATION

Anonymisation turns personal data into non-personal data and thus moves them outside the scope of the GDPR.[52] Note that the anonymization process as such is still under the scope of the GDPR. Alternatively, pseudonymised data is subject to the requirements of the GDPR because the ability to re-identify the individual exists, meaning that pseudonymised data is still personal data. It must be mentioned that anonymisation and pseudonymisation are distinct concepts and therefore the delineation of anonymisation and pseudonymisation need to be properly understood.

To determine whether personal data is identifiable Recital 26 of the GDPR provides that account should be taken of *all the means reasonably likely to be used* to identify the individual:

> *To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for*

[50] CJEU judgement of 19 September 2016 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779 Rz 25.
[51] GDPR, Article 4(2); Directive 2016/680, Article 3(2).
[52] GDPR, Recital 26.

> *identification, taking into consideration the available technology at the time of the processing and technological developments*.

Therefore, if data cannot be linked to a person by reasonable means, rendering them unidentifiable then the data is anonymous, and is no longer personal data and is consequently no longer subject to data protection legislation. In practice this means that it lies within the responsibility of the partner anonymising the personal data to assess which anonymising measures will be sufficient and which not.

The European Union Agency for Cybersecurity (ENISA) has been providing pseudonymisation guidance on state of the art pseudonymisation techniques to data controllers and processors since 2018.[53] They have just recently released a new report examining the technical methods for pseudonymisation to protect personal data. The report aims to help with specific use cases in such areas as information sharing in cybersecurity and can be helpful for partners to find the appropriate pseudonymisation techniques.[54]

As outlined above the line between personal data and non-personal data is increasingly becoming blurred. When it comes to AI in particular, controllers must be mindful that the unforeseen consequences of using a system designed to make connections and spot patterns not immediately visible to the human eye increases this risk of re-identification that was maybe not anticipated.[55] Whenever large data amounts of data are combined that appear not to be attributable to particular individuals in isolation the *'mosaic effect'* must be considered as there is *a* chance that they may cause a breach of privacy when combined.[56]

4.6.2 SPECIAL CATEGORIES OF DATA

The GDPR further makes a distinction between the processing of 'personal data' and the processing of 'special categories of personal data'. According to Art 9(1) GDPR, special categories of personal data include:

> *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.*

The processing of special categories of personal data is prohibited unless it is permitted according to one of the legal bases given in Art 9(2). Additionally, in line with Art 9(4) GDPR, one needs to take into account the national legislation, which might include additional requirements of processing genetic, biometric or health data.

In the application of the Law Enforcement Directive, Article 10 of the LED states the following for the processing of special categories of personal data:

---

[53] E.g. this report on pseudonymisation techniques and best practices https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices (accessed 04.02.2021).

[54] *ENISA*, Data Pseudonymisation: Advanced Techniques and Use Cases https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/ (accessed 04.02.2020).

[55] *CIPL*, Artificial Intelligence and Data protection: How the GDPR regulates AI (2020) (available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf (accessed 01.02.2021) page 4.

[56] *Pozen E. D.,* The Mosaic Theory, National Security, and the Freedom of Information Act (2005) The Yale Law Journal 115:3, Dec 2005, pp. 628-679. Available at: https://www.yalelawjournal.org/note/the-mosaictheory-national-security-and-the-freedom-of-information-act.

> *[…] shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:*
>
> *(a) where authorised by Union or Member State law;*
> *(b) to protect the vital interests of the data subject or of another natural person; or*
> (c) *where such processing relates to data which are manifestly made public by the data subject.*[57]

Additionally, and as pointed out by the WP29, '*Article 10 LED has to be read in connection with Article 8 LED.*' Therefore, the processing of special categories of data, if not foreseen by Union law, always requires a specific basis in national law (Article 10(a)), as defined by Recital 33. This specific legal basis has to meet the additional requirements set up by Article 10 LED. Compared with Article 8 LED the processing has to be *'strictly necessary'* and '*adequate safeguards'* have to be set up.[58] Article 8 LED only requires that processing be merely *'necessary',* whereas Article 10 in the processing of special categories of personal data requires that processing be ***'strictly necessary'.*** The distinction between these two interconnected legal provisions means that further consideration is required with Article 10 LED. In interpreting the meaning of *'strictly necessary',* the Digital Rights Ireland case can assist here. Specifically, the case states that:

> *So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.*[59]

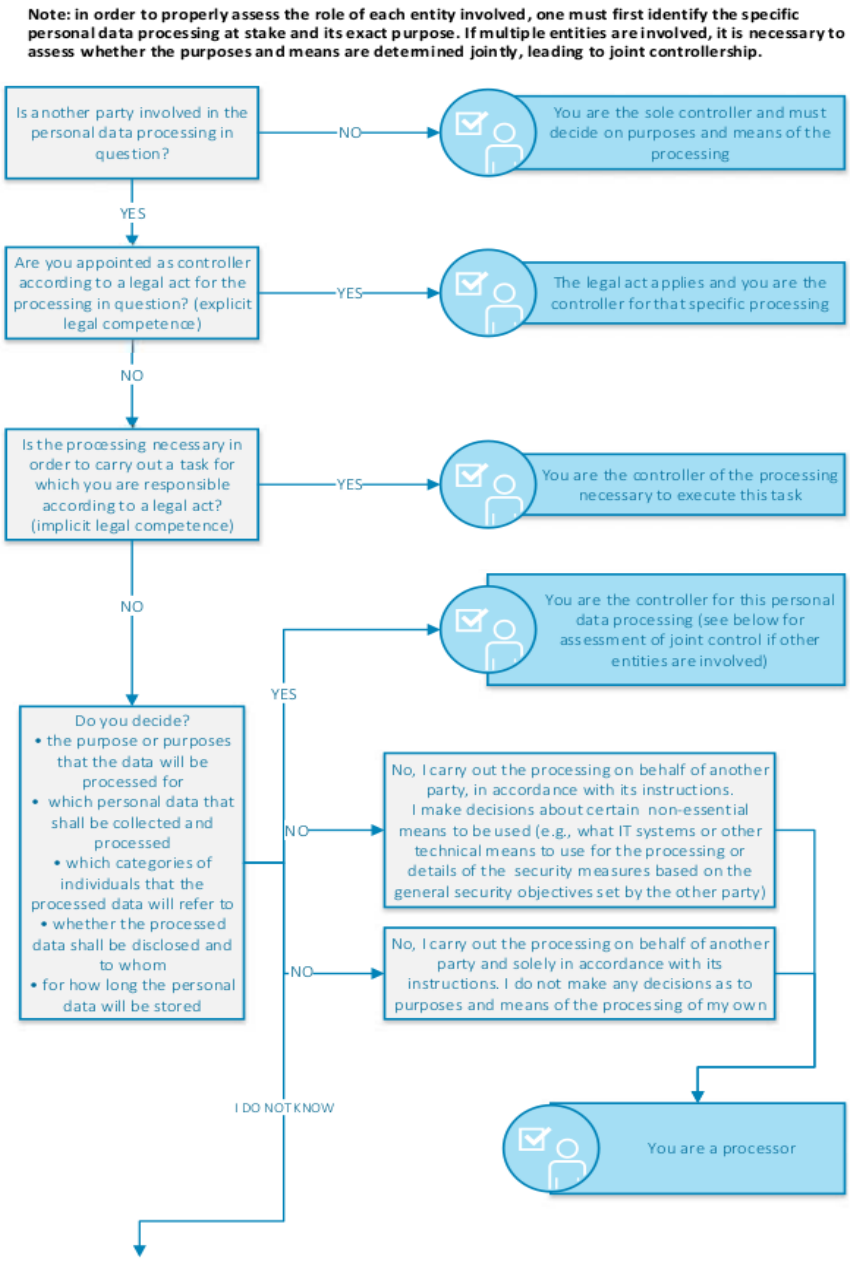
4.6.2.1 ROLES OF THE PARTNER

When processing personal data, the GDPR requires that entities processing that data assume either the role of the controller or the processor. The responsibilities of the controller are to adhere to all of the requirements of the GDPR including the principles of processing or ensuring the maintenance of data subject rights and demonstrate compliance. In delineation to the controller the 'processor' is *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*[60] In the words of the EDPB this means: *controllers and processors must seek to comply with the right to data protection in an active and continuous manner by implementing legal, technical and organisational measures that ensure its effectiveness*.[61] The role assumption depends on the circumstances, purposes and control of the data. Article 4(7) of the GDPR states that

'controller' means the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

[57] Directive 2016/680, Article 10.
[58] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on November 2017 page 7.
[59] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238, [52]; see also Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650, [92]; as for the use of a strict necessity test to assess legal measures.
[60] GDPR, Article 4(8).
[61] *EDPB,* recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (adopted on 10.11.2020), to be found here: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (accessed 11.01.2021) RZ 3, page 7.

Figure 3 Flipchart Controller Processor (1/2)[1]



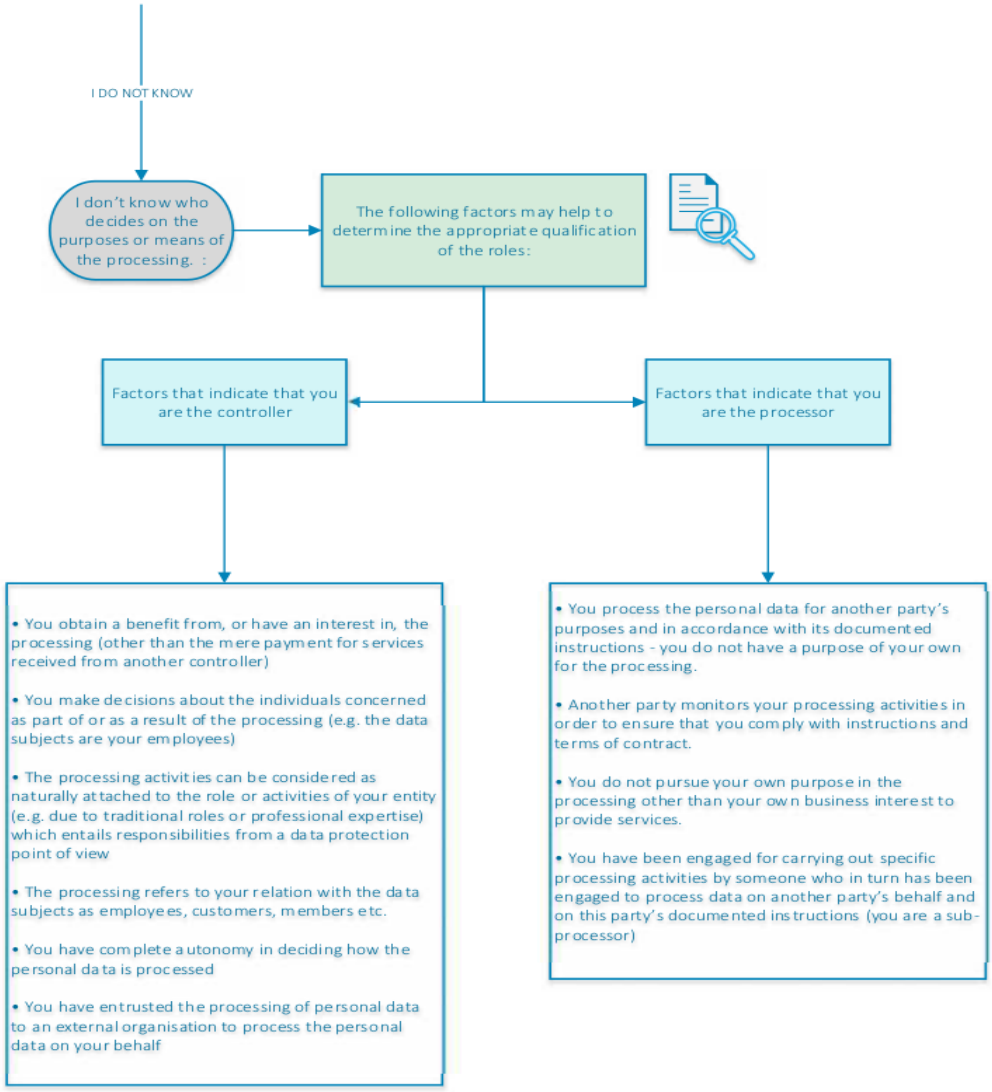
A distinguishing characteristic of controllers is that the controller determines the purposes and means of processing. As stated by the European Data Protection Supervisor (EDPS), 'the identification of the 'why' and the 'how' of a processing operation is the decisive factor for an entity to assume the role of 'controller' within the meaning of data protection law'.[62]

The Recently published guidelines by the EDPB regarding the concepts of controller and processor in the GDPR might additionally help the partners to identify their role (see the flowchart to the side and the following page).[63]

[62] *European Data Protection Supervisor*, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (EDPS, 7 November 2019) https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf (accessed 05.09.2020) page 9.

[63] *EDPB,* 'EDPB guidelines 07/2020 on the concepts of controller and processor in the GDPR' Version 1.0 (adopted on 02.09.2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (accessed 13.01.2020).

Figure 4 Flipchart Controller Processor (2/2) [64]



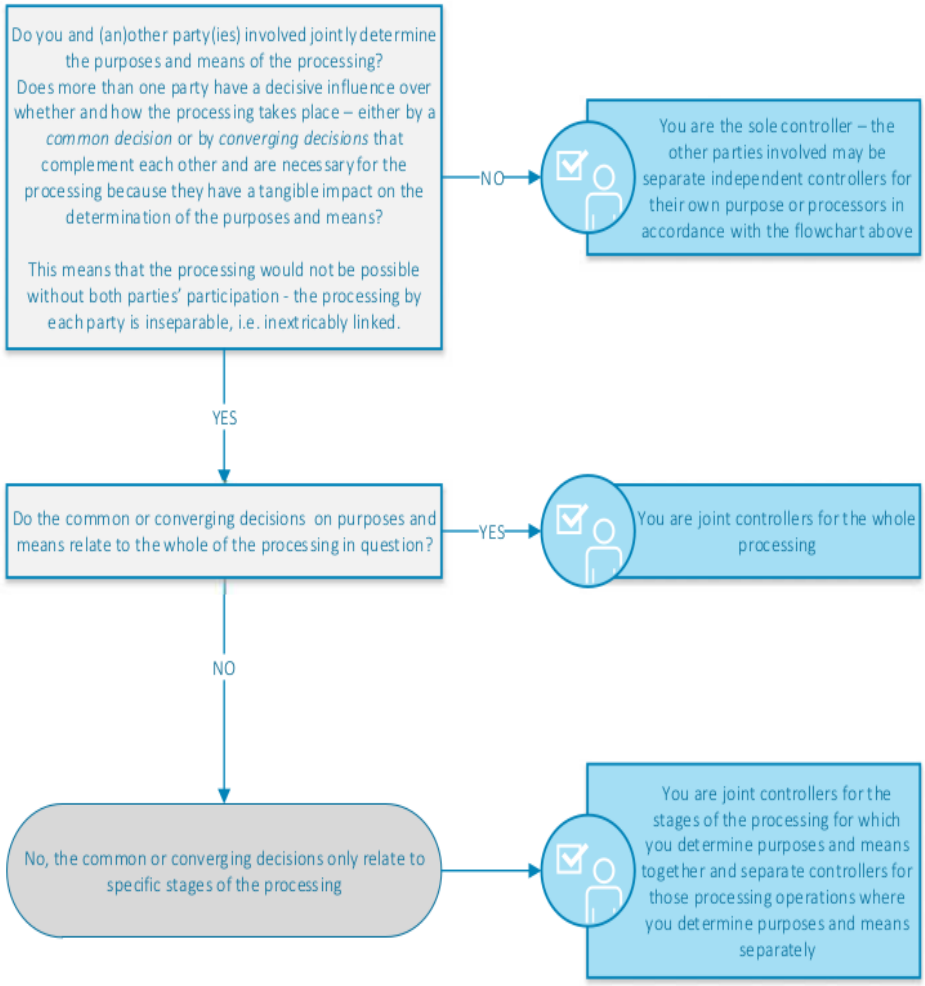
Article 26 also foresees the possibility of joint controllership:

> *Where* two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers *They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.* [65]

Furthermore, the EDPB provides a striking example on how joint controllership can be assessed that might help non-legal partners to comprehend the issue easily.

[64] European Data Protection Supervisor, 'EDPB guidelines 07/2020 on the concepts of controller and processor in the GDPR' Version 1.0 (adopted on 02.09.2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (accessed 13.01.2020) page 47.
[65] GDPR, Article 26(1).

Figure 5 Joint Controllership[66]



Example: Research project by institutes

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.[67]

Each partner organisation that fulfils the definition of data controller as defined in the GDPR will be individually liable for their compliance within the project. Due to the nature of the activities, there will be a number of joint controllerships and a joint controllership agreement needs to be put in place for those activities before the processing of personal data starts.

The LED differs slightly in its definition of what a controller is and states the following:

[66] *EDPB*, 'EDPB guidelines 07/2020 on the concepts of controller and processor in the GDPR' Version 1.0 (adopted on 02.09.2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (accessed 13.01.2020) page 48.

[67] *EDPB*, 'EDPB guidelines 07/2020 on the concepts of controller and processor in the GDPR' Version 1.0 (adopted on 02.09.2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (accessed 13.01.2020) page 21.

> *'controller' means* ***the competent authority*** *which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*[68]

The most notable difference between the two pieces of legislation is that the LED concerns the processing activities of the 'competent authority'. For the purposes of the Directive the controller must always be a 'competent authority' – this is not required within the GDPR. Article 3(7) of the LED provides two possible definitions of a 'competent authority':

> *(7)* ***'competent authority'*** *means:*
>
> *(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or*
>
> *(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;*

The principle commonality between (a) and (b) is the purposes of processing. The sameness here directly relates to and repeats the scope of the LED as set out in Article 1(1). Moreover, it is necessary it acknowledge the vagueness of who and what exactly a competent authority is. No precise organisations or entities are specifically named, and this is deliberate. As already mentioned, the LED requires national implementation, and as such public entities and law enforcement bodies differs between Member States, this definition provides a necessary amount broadness to encompass them all. This particularity should be taken into consideration when interpreting national implementation legislation.

Regarding the role of the processor Article 24(2) of the LED provides, that processors are obliged to maintain records of all categories of processing activities which have been carried out on behalf of the controller. Such records provide accountability on the side of the processor and controller, and if maintained correctly in accordance with Directive 2016/680, then such records protect the data subject as well as the data controller and processor when necessary. Further, with regard to operational measures, such records must be kept in writing – this includes electronic format. Moreover, the records must be made available to a supervisory authority upon request.

4.7 BASIC PRINCIPLES FOR PROCESSING PERSONAL DATA[69]

Article 5 GDPR provides the basic principles of data protection law and the processing of personal data. Intrinsic to keeping in line with data protection legislation is adhering to the core principles set out in the GDPR and correlating legislation (such as the LED[70] and the EU-DPR). Furthermore, the analysis of the principles is not only fundamental for this deliverable, but for the project as a whole because they will additionally help to uncover issues of the INFINITY solution at the development stage and will help include PET features in the architecture of the collaborative environment. The principles lie at the heart of data protection and partners,

[68] Directive 2016/680, Article 3(8).
[69] The ICO is providing an overview of the principles of data protection which can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (accessed 07.09.2020).
[70] Directive 2016/680, Article 4.

as well as the end-users, are guided by those principles and are requested to respect those principles whenever personal data is being processed. Respecting the spirit of those principles is also considered key to compliance with the detailed provisions of the GDPR. A failure to adhere to the following principles could lead to adverse legal effects such as civil liability, an administrative inquiry from the supervisory authority and administrative fines.

1. Personal data shall be:

> *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness**, **fairness** and **transparency**');*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**');*
>
> *(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');*
>
> *(d) 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 ('**accuracy**');*
>
> *(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation**');*
>
> *(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity** and **confidentiality**').*

*2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').*[71]

These principles will be briefly presented in an overview below to give the partners initial guidance in this matter.

4.7.1.1 ACCOUNTABILITY PRINCIPLE

The GDPR explicitly introduced in its Art 5(2) the accountability principle which is central to the legislation and pivotal for compliance. Accountability means that the controller shall be ***responsible*** and ***demonstrate*** compliance with the GDPR principles and requires data processors to establish and document data protection compliance processes. Data controllers, as described above in the 'roles of the partner' section, must implement appropriate and effective measures and be able to demonstrate compliance.

4.7.1.2 LAWFULNESS

[71] GDPR, Article 5.

A fundamental rule of European data protection legislation is the so called 'prohibition principle with reservation of permission'. This means that any processing is forbidden unless there is a specific legal basis that allows it. Article 6 of the GDPR provides an exhaustive list of possible legal bases.

As it will be explained later in this report, Informed Consent will constitute the preferred legal basis for all processing activities and will be sought whenever the nature of the processing is not contradicting that procedure. In all other instances where personal data in the sense of the GDPR will be processed a proper legal basis must be identified, such as for example 9(2)(j) which is of particular relevance to the project.

It must be considered that Art 6 and Art 9 GDPR are not the only possible sources of a legal basis for processing for the purpose of scientific research. Based on the opening clause in Art 9(2)(j) GDPR some EU Member States have introduced additional legislation with regard to processing of (special categories of) personal data for scientific research purposes.

A notable difference between the LED and the GDPR, relates to the consent of the data subject as one of the lawful grounds for data processing within the GDPR. Competent authorities should acknowledge that in the use of the LED and within the context of criminal investigation, consent from the data subject is not required since the processing of personal data might be necessary to comply with a legal obligation. One of the reasons being that consent under the GDPR should be freely given by the data subject, but the LED may require the data subject to comply with the legislation as a legal obligation.[72] Consequently consent is not provides as one of the bases for lawfulness of processing for purposes of the LED.

With further reference to the LED, one can refer to Article 8 of Directive 2016/680 which incorporates the necessity principle. As such, lawfulness of processing is enforced by the fact that '*processing is necessary for the performance of a task carried out by the competent authority for the purposes set out in Article 1(1) and that is it based on Union and Member State law*'.[73] In ensuring necessity, the competent authority must, if required, be able to show if necessary that data processing was the only adequate measure to achieve the aim of the law enforcement authority in relation to Article 1(1). In this instance as with the GDPR, the competent authority must consider '*the protection and vital interests of the data subject*'.[74]

4.7.1.3 FAIRNESS AND TRANSPARENCY

The GDPR does not provide a concrete delimitation of the notion of 'fairness' within the legal act. However, it is considered to mean that a controller must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. In the context of research projects, the question of fairness inevitably leads to the challenges of transparency and the informational balance and beyond that considering ethical aspects of data processing. The principle of transparency is additionally of special relevance for the development and deployment of AI.

Transparency can be described as being open and honest with the data subject and complying with the transparency obligations set out in Article 12-14 of the GDPR. Within INFINITY these requirements will be met on the one hand if personal data is directly collected from research participants, the Informed Consent and Information Sheets will be sought in an GDPR compliant format. In other instances, when for example large sets of online available personal data is not directly collected from the data subject, the controller will need to satisfy the requirements of Art 14 GDPR.

[72] Directive 2016/680, Recital 35.
[73] Directive 2016/680, Article 8.
[74] Directive 2016/680, Recital 35.

Articles 13 and 14 also set out various notice requirements specifying what individuals should be informed of before their personal data is processed. In the context of AI use, these notice requirements include an obligation to inform individuals of the purposes for processing, their rights in relation to their data and the existence of ADM, including meaningful information about the logic involved and the significance and envisaged consequences of such processing.[75] Furthermore, Recital 60 explicitly states that the data subject should be informed of the existence of profiling and the consequences of such profiling.

A notable point here is that the GDPR requires 'lawfulness, fairness and transparency'. The LED however omits the word 'transparency' – this exclusion is based on the purpose of processing. The fight against crime often makes use of sensitive data to which transparency would be counterproductive to a case and even potentially harmful to those involved. Therefore, as will be discussed in more detail further in this text, Article 15 of the LED stipulates that the right of access of the data subject may be subject to limitations. Nevertheless, within the context of the GDPR, transparency of data processing is primarily about '*engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes'*.[76]

However, adhering to transparent practices of data processing may be beneficial for both the GDPR and the LED as transparency can help provide verification and justification behind the purposes of data processing procedures and therefore help in demonstrating lawful and fair processing. This approach would assist in maintaining accountability on the part of the controller or processor. A practical example would be the maintenance of processing records: in a crime fighting context, this could simply mean ensuring transparency in evidence collection processes which is a fundamental aspect of relying on and presenting criminal evidence. Maintaining transparency in these processes so that they can be shown to the appropriate supervisory authority if required adds verifiable validity to the criminal evidence process, thereby providing legal certainty. As one commentator put it, '*this means that the lifecycle of digital evidence must always be accompanied by documentation, always kept up to date, constituting the so-called chain of custody*'.[77] Therefore transparency within this context would not mean that data processes would need to be shown to the data subjects in the case, but instead that for example the controller or processor could show that records are maintained regarding who accessed the data, when and where it was accessed and whether or not the crime data was altered in any way. Following the privacy by design approach as extensively outlined in D1.4 transparency in processing techniques such as the abovementioned can be foreseen in the structure of the INFINITY solution by implementing the appropriate technical solutions.

4.7.1.4 PURPOSE LIMITATION

The principle of purpose limitation is closely linked to the abovementioned. The principle of purpose limitation requires further that personal data will be collected only for '*specified, explicit and legitimate'* purposes and that data cannot be further processed for purposes that are incompatible with the one for which the data was originally collected. The requirements of *'specified'* and *'explicit'* prescribe that the purpose should be specific enough to prevent endless reusing of data and clearly communicated to the data subject (in line with the transparency requirement of Articles 12-14 GDPR).

---

[75] CIPL, Artificial Intelligence and Data protection: How the GDPR regulates AI (2020) (available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf (accessed 01.02.2021) page 16.

[76] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679. Adopted on 29 November 2017 (as last Revised and Adopted on 11 April 2018) page 4.

[77] *Biasiotti M. A.* and others, Introduction: Opportunities and Challenges for Electronic Evidence. in Maria Angela Biassiotti and others (ed), *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018) page 5.

Although the term "incompatible purposes" is not explicitly defined by the law, Art 6(4) provides guidelines on how to assess potential compatibility of two purposes and introduces the following criteria:

1. *any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;*
2. *the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;*
3. *the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;*
4. *the possible consequences of the intended further processing for data subjects;*
5. *the existence of appropriate safeguards, which may include encryption or pseudonymisation.*

Article 5(1)(b) GDPR does make an exception which is not included in the LED. The so called "compatibility presumption" excludes processing for purposes of archiving in public interest, scientific or historical research or statistics. Should any of the abovementioned be the secondary purpose for which data will be "further processed", then it shall "*not be considered to be incompatible with the initial purposes".*[78] This has to be in accordance with Art 89 GDPR and its national implementations. However, due to its complexity this topic provides some uncertainties and is on the EDPBs agenda.[79]

Article 9 of the LED regarding '*Specific processing conditions*' further solidifies the purpose limitation and provides details for its application. Article 4(1)(b) requires that processing only be done for the reasons set out in Article 1(1) of Directive 2016/680, unless specifically granted under Member State or EU law under which the GDPR would apply.

4.7.1.5 DATA MINIMISATION AND STORAGE LIMITATION

The principle of data minimisation stipulated in Article 5(1)(c) requires that the controller will only collect and process personal data that is necessary for achieving the legitimate purpose. Read together with the storage limitation (Art 5(1)(e) GDPR) principle they require that the controller erases personal data once they become obsolete in light of the declared purpose. It is therefore a duty of the controller to have implemented internal procedures that enable an ongoing monitoring of whether single datasets (pieces of personal data) are still necessary in light of the declared purpose or not. This duty of the controller is further developed in Art 17 GDPR (right to erasure).

4.7.1.6 ACCURACY

The accuracy principle as it is defined in Art 5(1)(d) of the GDPR requires that data shall be:

> *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 ('accuracy');*

[78] GDPR, Article 5(1)(b).
[79] EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (revised on 30.04.2020), to be found here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (accessed 13.09.2020), page 10.

This principle helps to ensure that data is accurate and true. If data is not accurate, then processing may not serve its intended purpose and it may even be detrimental to the data subject. This principle places an operational obligation on the controller and processor to ensure that data always accurate, and that any inaccuracies are amended. Controllers and processors have an obligation to the data subject and to the GDPR to adhere to this principle at all stages of processing activities.

4.7.1.7 INTEGRITY AND CONFIDENTIALITY

Article 5(1)(f) of the GDPR stipulates the principle of integrity and confidentiality and provides that personal data shall be:

> *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

This principle encompasses the requirements of the necessity of data security for legitimate data processing. Art 32 GDPR provides controllers and processors with further details as to how to adhere to this principle and ensure security of processing in general:

> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> > *a) the pseudonymisation and encryption of personal data;*
> >
> > *b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
> >
> > *c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
> >
> > *d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

Art 32 states the features of data protection which need to be taken into consideration when considering which types of security measures need to be put in place to sufficiently protect the rights and freedoms of the data subject. Art 32 also provides some examples of the types of security measures which could be implemented. However, neither do these examples constitute an exhaustive list of measures nor is a definition of the appropriate security measures provided. Rather, controllers must assess the potential risk of processing associated with the type, means and risks to the data subject and ascribe the appropriate security measures.

Given the nature of data, the integrity and confidentiality of processing requires particular attention. Data can be remotely and anonymously accessed, altered, stolen, observed etc. Such acts may negatively affect the processing and more importantly the data subject by presenting a risk to their fundamental rights and freedoms. A thorough and continuously monitored framework of implemented controls, both from the technical and organisational side can mitigate such possible adverse effects.

4.8 DATA SUBJECT RIGHTS

Individuals have certain rights in relation to the processing of their personal data under the GDPR[80], including the right of access,[81] the right to rectify or update their data,[82] the right to request erasure,[83] or the right to restrict or object to the processing in question.[84] Further, individuals have the right to receive the personal data they have provided to a controller in a structured, commonly used and machine-readable format.[85] As well as certain rights related to automated decision-making including profiling[86] (see below in more detail). Notwithstanding a few exception individuals can exercise their data subject rights and controllers as well as processors are obliged to enable the individuals the exercise of these rights to be in compliance with the GDPR.

As already elaborated above each Member State has the competence to introduce their own, national restrictions of certain data subject rights and especially the national implementations of Art 89 GDPR for the research context are monitored. In practical terms, this means that the exact scope of each right might differ between various Member States of the EU, and therefore between different consortium members and controllers.

[80] For further practical considerations consult for the example the ICOs homepage: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ (accessed. 17.02.2021).
[81] GDPR, Article 15.
[82] GDPR, Article 16.
[83] GDPR, Article 17.
[84] GDPR, Article 18, 21.
[85] GDPR, Article 20.
[86] GDPR, Article 22. LED, Article 11.

5 LEGAL FRAMEWORK FOR BIG DATA, AI AND AUTOMATED DECISION-MAKING

INFINITY foresees special tasks, especially within WP6, to use data mining, machine learning and artificial intelligence (AI/ML) techniques to cluster data, semantically analyse information and find links or patterns and aims to deploy Artificial Intelligence (AI) for the dual purpose of pattern identification and recommendations on enhanced data analysis and presentation.[87] The following section will therefore analyse the legal framework that is applicable to AI development and deployment and gives an outlook of the legal framework that is currently under development. Additionally, special considerations regarding how AI is governed by the GDPR will be made.

5.1 AI COMPREHENSIVE LEGAL FRAMEWORK ON AI?

At this point in time there is no comprehensive European legal framework covering Artificial Intelligence within the EU. However, the EC has published its long-awaited white book on AI regulation in February 2020: White Paper on Artificial Intelligence – A European approach to excellence and trust.[88] Hereby the Commission initiated a consultation of Member States civil society, industry and academics[89] and started the legislative process. The European Parliament has already adopted three resolutions on AI, one covering ethical principles for the development, deployment and use of AI.[90] A report from the Committee on Civil Liberties, Justice and Home Affairs (LIBE) on Artificial Intelligence in criminal law[91] is still in preparation. A first proposal for a draft legislation by the Commission is expected in early 2021 which will only be one of the first steps in a likely multi-year process that will lead to a regulation coming into effect.

The ECs approach to an AI regulation is to embrace the possibilities this technology brings, while managing the risks of AI applications. The EDPS urged the European Commission to advocate the strict application of a precautionary approach as outlined in its opinion.[92] The EC proposed a risk-based approach that 'high risk AI' will be under a different regulatory regime than those that are identified as non-high risk. Even though the criteria cannot be anticipated, the deployment of AI by law enforcement would undoubtedly fall under the umbrella of high-risk AI, considering sector and use of the deployment and the human rights sensitivity of law enforcement operations. The White Paper, strongly considering the 'Ethics Guidelines for Trustworthy Artificial Intelligence' by the AI HLEG, introduced six key requirements (for high-risk AI) which could be an essential part of AI regulation: Training data, data and record-keeping, provision of information, robustness and accuracy, human oversight and specific requirements for certain AI applications, such as remote biometric identification.

[87] INFINITY Grant Agreement (883293).
[88] *EC*, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020).
[89] The results of the consultation process can be found here: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence (accessed 06.02.2020).
[90] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.pdf (accessed 01.01.2021).
[91] LIBE, Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) to be published here https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2016(INI)&l=en.
[92] EDPS, Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust (2020) https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf

[93] However, the outcomes of the legislative process can and should not be anticipated and as we still lack a draft proposal these considerations do not yet constitute legal obligations, but rather ethical guidance as discussed in the following section.

Regarding more concrete legal proposals that are yet to be transformed into binding norms we can already consider the proposal for the Europol Regulation. The new proposal suggests a paragraph that can already guide the research as this might be a legal obligation in the future:

Europol shall keep a complete and detailed description of the process and rationale behind the training, testing and validation of algorithms to ensure transparency and for verification of the accuracy of the results.[94]

5.2 AI AND THE GDPR

Even though a comprehensive legal framework is yet to be established we do not find ourselves in a legal vacuum. Quite the opposite is the case. Developers and deployers of AI are already subject to European and national legislation ranging from consumer protection, product safety and liability and for the INFINITY project of utmost importance, fundamental rights (first and foremost data protection, privacy and non-discrimination). The so-called 'European approach to AI'[95] must be grounded in EU values and fundamental rights ranging from human dignity, equality, the rule of law, pluralism, due process and especially the protection of privacy and personal data and therefore respect the European data protection acquis in its entirety. The GDPR has been developed as a technology neutral legislation that is capable of responding to new, evolving and emerging technologies such as AI. It is apparent that Artificial Intelligence requires access to big data, including the use of personal data in terms of the GDPR and corresponding legislation outlined in this report. The EDPB has emphasised the self-evident fact that '*any processing of personal data through an algorithm falls within the scope of the GDPR.*'[96] Therefore the entirety of the provisions analysed within this document and outlined in European data protection legislations need to be adhered at every point of development and deployment. General considerations have been already made in the analysis provided in the sections above. Some GDPR provisions and considerations are of special relevance and will be reiterated and further analysed in the following subsection.

5.2.1 PROFILING AND AUTOMATED DECISION-MAKING

The GDPR (Art 22) as well as Directive 2016/680 (Art 11) prohibit automated individual decisions that are made without human involvement or intervention in the decision-making process ('solely automated decision-making'). Due to the inherent differences in the scope of application of the two instruments, the prohibitions for ADM and profiling are not identical despite some similarities. Art 22(1) GDPR for examples introduces three possible exceptions from the general ban:

[93] EC, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020).
[94] Proposal ER, Art 33a(3).
[95] As prominently invoked by the EC in its White Paper on AI regulation.
[96] *EDPB*, Response to an MEPs letter on unfair algorithms, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf (accessed 17.02.2021).

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c) *is based on the data subject's explicit consent*.[97]

The Directive on the other hand does not recognize the exceptions to the prohibition mentioned in the GDPR, but on the other hand requires that such a decision has 'adverse' legal consequences or otherwise 'significantly affects' them. The former Article 29 Working Party has already provided guidelines on automated individual decision-making and profiling in the scope of the GDPR.[98] However, the FRA believes that the concept of automated decision making is elusive and therefore requires further discussion and research.[99] The applicability of this provision might not even be of relevance since the intended use of AI will only be developed to assist the investigator in the decision-making process. Depending on the technical progress of the project the particular issue will be reassessed. The human intervention has to suffice the requirement of being qualified, capable of discovering and recovering unfair outcomes or discriminations, as the EDPB has recently pointed out in its guidelines on data protection by design and by default.[100]

5.2.2 DATA MINIMISATION

The tension between the principle of data minimisation and the fact, that algorithms need to be trained by a substantial amount of data to be efficient, may seem apparent. AI systems may not be able to perform without first being trained on large data sets. Additionally, simply maximizing the amounts of data to feed into the algorithm entails to increases the risk of possibly unlawful data collection practices, especially regarding secondary processing. However, the concepts of Big Data and Machine Learning are not incompatible with the principle of Data Minimisation. The principle itself does not limit the processing of data by way of reference to a specific volume or set of data elements, but it refers to what is 'necessary' for the purposes of the processing. What personal data is considered 'necessary' varies depending on the AI system and the objective for which it is used. The level of accuracy that is required is to be a determining factor in the selection of data elements for inclusion. Additionally, as best practices it was suggested that controllers should set limits that are sufficient to achieve the purpose of the processing, rather than using all available data.[101]

5.2.3 DATA PROTECTION IMPACT ASSESSMENT

Art. 35 GDPR provides the concept of a Data Protection Impact Assessment:

[97] GDPR, Article 22(2).
[98] *Article 29 Working Party,* Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, WP251rev.01, As last Revised and Adopted on 6. February 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (accessed 23.11.2020).
[99] FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement (2019) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (accessed 22.11.2020).
[100] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (13 November 2019) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (accessed 12.02.2021).
[101] CIPL, Artificial Intelligence and Data protection: How the GDPR regulates AI (2020) (available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf (accessed 01.02.2021) page 13.

> *1. 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, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

The reference to 'the rights and freedoms' of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion as this was also reiterated by the EDPS opinion on the AI White Paper.[102]

The Art 29 Working Party considers a Data Protection Impact Assessment as a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance. [103]

A DPIA can be considered necessary if for example the processing could affect a large number of data subjects and is likely to result in a high risk to the rights and freedoms of the data subject, especially when using new technologies. The use or development of an algorithm can trigger the obligation to carry out a DPIA prior to any processing taking place. The ICO highlights that AI, machine learning and deep learning are to be considered as innovative technologies that likely trigger the requirement for a DPIA in terms of Article 35 GDPR.[104] Even in cases where the GDPR does not require the controller to conduct a DPIA, it is good practice to conduct such an assessment in order to ascertain and minimise risk wherever the envisaged data processing is complex, large-scale or sensitive. All partners are encouraged to carry out DPIAs whenever this is deemed necessary.

If the outcome of the DPIA indicates that the processing would, in the absence of measures, result in a high risk, the controller will have to consult the relevant supervisory authority prior to the processing. The outcome of the assessment can also be that the controller will have to refrain from using a specific algorithm, or parts of it, if the risks to the rights of data subjects and other persons cannot be sufficiently mitigated.

[102] European Data Protection Supervisor, 'EDPS Opinion on the European commission's White Paper on Artificial Intelligence – A European approach to excellence and trust' (29 June 2020) https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf (accessed 19.02.2021) page 15.

[103] *Article 29 Data Protection Working Party*, Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, (as last revised and adopted 4 October 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[104] I*CO*, Guidance on DPIA https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when4 .

6 ETHICAL AND SOCIETAL FRAMEWORK

As it was already elaborated in D1.4 and the SHIELD framework, the application of advanced and (semi-)automated big data analytics in LEA investigations complexifies the regulation of responsible development and use of these technologies due to considerations of accountability, transparency and acceptance by the public.[105] Therefore, besides legal compliance also the ethical dimension plays an important role. Special attention should be paid to ethical codes that could have a strong impact on possible future legislation, such as the AI HLEG and those that have been developed by the EC in regards to H2020 or similar research projects.[106]

6.1 ETHICAL RESEARCH

Art. 19 of the Regulation establishing Horizon 2020 provides that any research and innovation activities carried out under Horizon 2020 shall not only comply with relevant national, Union and international legislation but also the relevant ethical principles.[107] Art. 34 of the INFINITY Grant Agreement reemphasizes the obligation that all beneficiaries need to be in compliance with ethical and research integrity principles.[108] Failing to incorporate these values would not only indicate irresponsible research that results in outputs of questionable value that may be seen as unreliable and high-risk but would also constitute a breach of a beneficiary with the abovementioned obligations and may lead to significant adverse effects.

Therefore, the INFINITY consortium considers ethics as an integral part of research from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence. Ethical compliance will furthermore facilitate public trust in the solution and increase credibility in the project's outputs.

While there are specific data protection and human rights laws with normative effects to protect individuals, that this project will fully adhere to, there are no specific laws regarding ethics. To put in the words of the European Data Protection Supervisor: Ethical thinking and deliberation come before, during, and after the law.[109] The fact that our research is legally permissible does not necessarily mean that it will be deemed ethical. Therefore, the responsibility lies within each participating partner to conduct their tasks in ways that include respect and protection of human values, which are intrinsic to the existing legislation and fully adhere to the highest ethical standards, as set out for example in The European Code of Conduct for Research Integrity.[110]

6.1.1 THE EUROPEAN CODE OF CONDUCT FOR RESEARCH INTEGRITY (ALLEA)

[105] *Joh EE* (2015) The new surveillance discretion: automated suspicion, big data, and policing. Research Paper No. 473, *UC Davis Legal Studies Research Paper Series*, December.
[106] E.g.: EC, Ethics in Social Science and Humanities (2018) https://ec.europa.eu/info/sites/info/files/6._h2020_ethics-soc-science-humanities_en.pdf (accessed 03.02.2021); EC, Ethics and Data Protection (2018) https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf (accessed 10.01.2021).
[107] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC Text with EEA relevance [2013] OJ L 347/104.
[108] INFINITY Grant Agreement (883293).
[109] To be found here: https://edps.europa.eu/sites/edp/files/publication/19-03-25_reuters_interview_en.pdf (accessed 20.08.2020).
[110] ALLEA - All European Academies, The European Code of Research Integrity (2017) https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf (accessed 23.08.2020).

Research ethics can be described as a set of standards that affords protection to all those involved in the research, whilst maximising the value and benefits of the endeavour. INFINITY will adhere to the highest ethical standards throughout the research and development process. As already mentioned above ethics was introduced as a fundamental key within the EU's H2020 Research and Innovation Programme. The European Code of Conduct for Research Integrity aims to guide researchers in their work with the practical, ethical and intellectual challenges of the research process and describes good research practices for research activities.

The partners will be guided by the fundamental principles of The European Code of Conduct for Research Integrity foundational framework for research activities. These principles are the following:

- **Reliability** in ensuring the quality of research reflected in the design, the methodology, the analysis and the use of resources.
- **Honesty** in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair and unbiased way.
- **Respect** for colleagues, research participants, society, ecosystems, cultural heritage and the environment.
- **Accountability** for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.

This will include the selection of human participants and pilot scenarios to avoid potential biases. Moreover, the Consortium will undertake every possible measure to mitigate the potential for misuse of the research findings or technical outputs.

6.1.2 ETHICAL CONSIDERATIONS FOR INFINITY

During the ethical self-evaluation process and the ECs ethics review the most important ethical issues for the INFINITY project were identified. This concerns research involving human beings (the participation of volunteers), the protection of personal data , misuse of research findings and transfers of materials. The identified requirements for ethical compliance have been added into the GA as a separate Work Package to tackle these issues. While WP11 addresses these issues that stem from human involvement (recruitment, vulnerable groups, etc.), data protection, research materials and potential misuse, particular additional consideration will be made to issues pertaining to big data, automated processing utilising AI and ML and the potential use of cloud infrastructure. Legal and ethical risk assessments will be carried out in WP2 leading to recommendations so that should an ethical or legal issue which have not been already anticipated arise the consortium will be in a position to introduce effective countermeasures. Effective countermeasures means, among others, that we can live up to the responsibility to produce a system that has features built in, that automatically protect individuals' legal and ethical rights by default. Due to the nature of the project, public trust and confidence is of the utmost importance.

6.1.3 ADDITIONAL ETHICAL DIMENSION OF DATA PROTECTION

Data protection is not only a fundamental human right but also a central issue for research ethics. While all partners must comply with EU and national data protection laws, the consortium is additionally guided by ethical considerations that are intrinsic to privacy and human dignity. Partners can additionally consult the EC

report and Ethics and Data Protection[111], that was specifically drafted to guide beneficiaries of EU research projects in the intersection of ethics and data protection.

6.1.3.1 SECONDARY PROCESSING

The GDPR provides for a distinction to be made between primary and secondary processing of personal data as the different types of processing have significant consequences which are not only legal but also ethical. The distinction between scientific research based on primary or secondary usage of personal data will become particularly important when considering the legal basis for the processing, the information obligations and the purpose limitation principle pursuant to Article 5(1)(b) GDPR.[112]

Secondary processing refers to situations where personal data collected for one purpose, are being used for another one. In the context of INFINITY secondary processing means using personal data collected before the start of the project for different purposes to be used to develop the INFINITY solution. As it was indicated in the GA that some partners might be engaged in secondary processing of personal data (e.g. LEAs) they would need to identify an appropriate legal basis for such processing. Should such a basis be lacking, secondary processing would need to be considered unlawful in light of the GDPR.

Additionally, as stated in Recital 156 GDPR processing for secondary purposes requires additional safeguards from the controller, such as pseudonymisation or other technical and organisational measures that would ensure that the principle of data minimisation as outlined above is followed. If there is the intention to use datasets including personal data that were collected for example from a previous research project, the beneficiary must provide details regarding the initial data collection, methodology and informed consent procedure of the primary data collection. The partner must also confirm that they have permission from the owner/manager of the dataset to use the data in the project.

6.1.4 HEALTH AND WELLBEING CONSIDERATIONS

Health and wellbeing considerations will play a key role in the research and development of INFINITY. From a cognitive point of view, although stereoscopy provided by VR equipment may induce visual fatigue, 3D rendering and immersion in a virtual environment are suggested to contribute to the reduction of cognitive load, therefore contributing to increased performance in tasks. Some parameters are known to improve the benefits, such as embodiment of the participants with avatars, control of the avatars and reduction of disturbance from the environment so that the user can optimise their flow. T2.1 and T2.2 will undertake to identify the optimal health and safety procedures that will inform the development of INFINITY as well as guidelines for usage. This will minimise the side effects of prolonged immersion while retaining the cognitive benefits on performance and comprehension.[113]

6.1.5 INFORMED CONSENT

[111] EC, Ethics and Data Protection (2018) https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf (accessed 10.01.2021).
[112] EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (revised on 30.04.2020), to be found here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (accessed 13.09.2020) page 6.
[113] Reference to INFINITY Grant Agreement (883293), page 178.

In terms of the GDPR, Informed Consent is a *freely given, specific, informed and unambiguous indication*[114] from the data subject (the research participant) that he or she agrees to the processing of his or her personal data. Moreover, Informed Consent is one of the most pivotal principles in research ethics (not limited to medical research) and guarantees the voluntary participation of the individual to the research activity. The aim of Informed Consent can be considered to be twofold, having a legal and an ethical dimension.

As already discussed in D1.4, as result of a good and ethical research practice Informed Consent should and will constitute the preferred legal basis for all processing activities in INFINITY and will be sought whenever the nature of the processing is not contradicting that procedure. This is especially the case for research activities that foresee a direct involvement of human research participants, such as the pilots and surveys foreseen in WP9.

D11.2 reported on the concrete procedures for recruitment and Informed Consent that are foreseen whenever direct human involvement is conducted within INFINITY. The partner's DPOs play an important role to ensure compliance and to establish the effective audit trail of the process deployed for obtaining consent. Within D11.3 the beneficiaries are currently in the process of being asked to provide a confirmation of the appointment and the contact details of their host institutions DPO.

6.1.6 POTENTIAL MISUSE OF RESEARCH FINDINGS

Some aspects of the INFINITY research involve materials, methods or technologies or generates knowledge that could be misused and be of potential harm for human beings. Not only the immediate aims and intended applications of INFINITY need to be considered, but also whether our research could serve unethical purposes. Although the research is carried out with benign intentions the potential misuse, such as the leakage of confidential methods of techniques employed by law enforcement agencies, cannot be completely eliminated. However, by recognising the risks in good time and taking the right precautions, such as the establishment of the Security Advisory Board, and employing a risk-based approach, any potential harm can be mitigated. As it was already pointed out in the GA 'the security levels and locations of the various components will render the opportunity for misuse extremely unlikely' [115]. Further elaborations regarding risk assessment and details on measures to prevent misuse of research findings can be found in D11.5.

6.1.7 AI WHITE PAPER AND THE HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE

The High-Level Expert Group on Artificial Intelligence has produced Ethics Guidelines for Trustworthy AI which will be considered throughout all phases of the development of the INFINITY project. The guidelines have provided three components and six key requirements, which should be met throughout the system's entire life cycle. Three components:

(1) it should be **lawful**, complying with all applicable laws and regulations
(2) it should be **ethical**, ensuring adherence to ethical principles and values and
(3) it should be **robust**, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm.[116]

Obviously, even though the principles developed bv the AI HLEG are not limited to data privacy and aim to address a broader set of concerns arising from this technology, they overlap in various ways with the GDPR

[114] GDPR, Article 4(11).
[115] Reference to INFINITY Grant Agreement (883293), page 178.
[116] To be found here https://ec.europa.eu/futurium/en/ai-alliance-consultation (accessed 27.08.2020).

requirements and even draw from the GDPR concepts. For example, they emphasise respect for human autonomy, and specifically human agency and associated rights as key requirements when using AI.

The CIPL developed a table in its report that shows the overlap between the seven key requirements of the AI HLEG Guidelines and the requirements of the GDPR. The table exemplifies the extent to which GDPR concepts have inspired the principles of trustworthy AI and will likely shape the upcoming AI Regulation as outlined above.

Figure 6 CIPL AI and GDPR table [117]

Key requirements of Trustworthy AI	Overlap with GDPR provision
Human Agency and Oversight	• Legitimate interest balancing test (Art. 6(1)(f)) • Transparency (Art. 13 & 14) • ADM (Art. 22) and Right to obtain human intervention (Art. 22(3)) • Risk assessment and DPIA (Art. 35)
Technical Robustness and Safety	• Security (Art. 32) • Risk assessment and DPIA (Art. 35) • Data accuracy (Art. 5(1)(d))
Privacy and Data Governance	• Data protection principles (Art. 5) • Legal grounds for processing (Art. 6) • Legal grounds for sensitive data (Art. 9) • Rights of the data subject (Chapter III) and in particular Transparency (Art. 13 & 14); Right to information on ADM and logic involved (Art. 15(1)(h)); Right not to be subject to an ADM decision (Art. 22) and Right to human intervention (Art. 22(3)) • Accountability (Art. 5(2) & Art. 24(3)) • Data protection by design (Art. 25) • Processor due diligence (Art. 28(1)) • Security (Art. 32) • DPO (Art. 37 & 38)
Transparency	• Transparency (Art. 13 & 14) • ADM (Art. 22)
Diversity, Non-Discrimination and Fairness	• Fairness data protection principle (Art. 5.1(a)) • Risk assessment and DPIA (Art. 35) • Right to information on ADM and logic involved (Art. 15(1)(h))
Societal and Environmental Wellbeing	• Risk assessment and DPIA (Art. 35) • Transparency (Art. 13 & 14)
Accountability	• Accountability (Art. 5(2) & 24(3)) • Risk assessment and DPIA (Art. 35) • Processor due diligence (Art. 28(1)) • DPO (Art. 37 & 38)

6.1.8 BIG DATA, OPACITY, THE BLACK BOX EFFECT AND ALGORITHMIC BIAS

The areas of Artificial Intelligence, surveillance by authorities and automated decision-making are all highly contentious and ethical norms are in the process of being established. The deployment of AI inherently entails the risk of unjustified discrimination of the persons affected by the decision. The dogmatic discussion on

[117] CIPL, Artificial Intelligence and Data protection: How the GDPR regulates AI (2020) (available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf (accessed 01.02.2021) page 18f.

algorithmic discrimination is still in its infancy.[118] INFINITY will be mindful of particular concerns in the sphere of big data, predictive analytics and artificial intelligence that cross legal, ethical, societal and privacy boundaries and intends to contribute to the debates, by demonstrating that ethical standards can be incorporated in these practices. It is important to understand the ethical dimension of these issues, as the AI HLEG puts it:

*'[…] even after compliance with legally enforceable fundamental rights has been achieved, ethical reflection can help us understand how the development, deployment, and use of AI may implicate fundamental rights and their underlying values, and can help provide more fine-grained guidance when seeking to identify what we **should** do rather than what we (currently) **can** do with technology.'*[119]

Known issues, such as the black box effect might have detrimental impact on individulas or society as a whole. Black box means that algorithmic decision making is not comprehensible. This can either stem from intransparency and invoking of business secrecy or the sheer complexity of the information processing that the AI is conducting. These issues raise several questions not only in the domain of fundamental rights protection but also for ethical development of such technologies.

Whenever large amounts of data are to be processed, we as researcher have to be mindful of the fact that behind these data engages with human individuals.

'[…] all these data are people. As a researcher you have the ethical responsibility to minimise potential harm to them.'[120]

6.2 SOCIETAL IMPACT

As the data protection acquis and fundamental rights specifically aim to protect the rights of individuals, additional attention should be paid to the broader societal implications of newly developed technologies that may exceed the individual sphere. For example, even if research is conducted with anonymised data sets and data protection adherence is given, it may *cause harm to a group through, for instance, discrimination against or stigmatisation of entire populations.*[121] The societal impact assessment helps to identify the societal needs, define the societal benefits and monitor potential negative implications of the research outputs for broader society. This subsection provides an initial assessment and input for considerations regarding the societal impact of the INFINITY solution. A first complete societal impact report of INFINITY will be provided within D1.7 and will be followed up and complemented with D2.5 considering the progress of the project.

New technologies, such as those developed within INFINITY are at the service of all Europeans – improving their security while respecting their rights. The EC considers Europe's current and future sustainable economic growth and societal wellbeing dependent on value created by data. AI development is still in its early stages which entails that there is a lack of full view of its impact on our society. *Given the major impact that AI can*

[118] Peters in Kaulartz/Braegelmann Rechtshandbuch Artificial Intelligence und Machine Learning (2020), Strafrecht page 559ff.
[119] Ethics Guidelines for Trustworthy AI, to be found here: https://ec.europa.eu/futurium/en/ai-alliance-consultation (accessed 27.08.2020) Rz 40.
[120] Matthew Zook et al. (2017). Ten simple rules for responsible big data research. Editorial. Plos Computational Biology, March 30, 2017, available at: http://journals.plos.org/ploscompbiol/article/file?id=10.1371/journal.pcbi.1005399&type=printable.
[121] *Pozen E. D.,* The Mosaic Theory, National Security, and the Freedom of Information Act (2005) The Yale Law Journal 115:3, Dec 2005, pp. 628-679. Available at: https://www.yalelawjournal.org/note/the-mosaictheory-national-security-and-the-freedom-of-information-act.

have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection.[122]

The impact of AI technologies exceeds the individual sphere and must be considered from a wider societal perspective. The EC has acknowledged that AI technologies have the potential to serve both citizens and the public interest. For example, equipping law enforcement authorities with appropriate tools provides an opportunity for better protecting EU citizens from crime and acts of terrorism and ensure the security of citizens.[123]

The societal need that INFINITY aims to address is to increase the capacity and efficiency of operations targeting terrorists and cybercriminal groups by enhancing LEA capabilities. These considerations were already made extensively on the outset of the project in the GA preparation phase: The threats of cybercrime and terrorism are high and include fear of attack or loss of property; perceived loss of freedom; deterring positive use of technology; distrust in specific groups (whether professions or communities); undermined social, political and economic cohesion; loss of trust in institutions (linked to perceived inability to tackle those threats) and legitimate calls for public action. Despite the major steps taken since 2015 to improve the response to terrorism, the threat remains high. Cybercriminal activity intersecting with a plethora of other threats, including terrorism, is also growing facilitated by the new communication opportunities offered by online service platforms. Through improving the usability of complex, heterogenous and distributed datasets, more efficient and effective decision-making on operational and tactical levels and improved collaboration between investigators of different MS, INFINITY will directly contribute to improving the common European response to these threats thus disrupting the activities of criminals and terrorists, reducing the risks to society and addressing the concerns of the EU citizens. Strengthening the fundamental human rights to life, liberty and security by targeting conditions favourable to perpetrators of cybercrime and terrorism who actively seek to violate these fundamental rights. The enhanced capabilities of LEAs will have direct positive impacts leading to a safer and more secure society for European citizens by improving the usability of complex, heterogenous and distributed datasets. Additionally, it will enable more effective decision-making on operational and tactical levels and improve collaboration between investigators of different Member States. Developing better standards and procedures that improve information sharing and collaboration amongst MS LEAs can decrease reliance on ad-hoc procedures and cut out inefficiencies. Enhanced collaboration across MS LEAs also benefits territorial cohesion across EU Member States. Ultimately INFINITY aims address the societal need of safeguarding European citizens by more efficiently fighting crimes that undermine the fabric of society.[124]

The societal benefit of INFINITY can be derived from that needs assessment. The cutting-edge tools developed by INFINITY will significantly increase the analytical and investigative capabilities of LEAs in the field leading to faster response times to emerging threats, increased capacity to investigate and pursue targets and resultantly increase protection against existing and horizons threats and societal vulnerabilities. A further principle objective of INFINITY is to achieve short-, mid- and long-term positive societal impacts by improving Member States LEAs capabilities to acquire, integrate, visualise, annotate and shape information from open and LEA proprietary sources using virtual/augmented reality within an advanced collaborative environment to prevent and fight terrorism, cybercrime and hybrid threats.[125] Enhanced LEA capabilities to handle heterogenous and distributed data sources in an advanced VR/AR supported collaborative environment will serve specifically

[122] EC, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020) page 2.
[123] EC, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020) page 1f.
[124] INFINITY Grant Agreement (883293).
[125] INFINITY Grant Agreement (883293).

people vulnerable to cybercrime and terrorism by increasing the likelihood of criminal actors and activities to be identified. Moreover, reducing the time and personnel costs of legal investigations and making more efficient use of LEAs resources, are also considered as a societal benefit. INFINITYs innovations will have a positive impact on society as a whole by improving the ability of LEAs and other agencies to address terrorists and cybercrime threats as well as attacks on vital infrastructures. Critically improved visualisation and collaboration abilities will update existing LEA abilities to identify relevant actors as well as current and emerging threats. The early detection of threats supports the safeguarding of European citizens as a whole as it enables LEAs to identify plots for terrorist and detect terrorist and cybercrime networks. Improving the ability of LEAs to identify perpetrators, networks and criminal activities removes the threat and results in a safer society for all citizens. Enhancing LEA capabilities to remove serious crime threats and safeguard citizens from terrorism and cybercrime fosters human dignity broadly.

Besides the abovementioned extensive societal benefits also the potential negative impact on society as a whole need to be scrutinized. There are inevitable concerns attached to the use of new technologies that are inherent to their usability. In the case of AI applications for law enforcement and the judiciary citizens' rights may be most directly affected and compliance with EU legislation, principles and values is of particular relevance. INFINITY will make use of heterogeneous, distributed data from open and privileged sources and powerful visualisation and integration capabilities to analyse, annotate and interpret these data sources. Such activities have the potential to be intrusive, i.e. pose a risk specifically in terms of privacy and data protection as enshrined in the CFR. If the capabilities of the technology were misperceived by the public, potential negative effects such as chilling effects could be possible. In the context of LEA technologies, ethical risks have been identified with regard to '*accidental discrimination, the Mosaic effect, algorithmic opacity, data aggregation with mixed levels of reliability, data and reasoning provenance, and various biases'*.[126] Within INFINITY AI elements will support VR/AR functionalities and support the decision-making process of investigators. Big Data and AI/ML methodologies have to potential for biases in the data sources and/or algorithmic models. Biases based on gender, race and ethnicity have already been identified in the past.[127] It would not therefore be surprising if such a technology were to exacerbate social biases when used by LEAs.[128] These biases could disproportionally affect groups that historically have been policed more heavily perpetuating historical biases. Further, selection biases in training and test data can lead to discriminatory interpretations or decisions (e.g. women, elderly, disabled people, ethnic minorities, non-English speakers, etc. which tend to be under-represented in data sets).

LEAs should maintain awareness as to the assistive nature of the tool. Overreliance could lead to profiling and discrimination of entire neighbourhoods and ethnic groups. In lacking this awareness, traditional policing practices could potentially but drastically change, whereby any data collected would be '*used for predictive, rather than reactive or explanatory, purposes'*.[129]

[126] *Duquenoy P*. and others, Addressing Ethical Challenges of Creating New Technology for Criminal Investigation: The VALCRI Project. in Georgios Leventakis and MR Haberfeld (eds), Societal Implications of Community-Oriented Policing and Technology (Springer Open 2018) 35.
[127] E.g. *Andrew D. Selbst*, 'Disparate Impact in Big Data Policing' (2017) 52 Georgia Law Review 109-195.
[128] *Jo Goodey*, 'Migration, crime and victimhood: Responses to sex trafficking in the EU' [2003] 5(4) Punishment & Society 415-431.
[129] *Brayne*, 'Big Data Surveillance: The Case of Policing' (2017) 8(5) American Sociological Review 977- 1008.

7 CONCLUSION

This report provides an **initial analysis of the relevant legal, societal and ethical framework** that INFINITY operates in. The report will contribute to the overarching aim of WP2 to provide legal and ethical analysis in relation to activities taking place during the project, as well as for post-project end use of the system by LEAs in real-life scenarios.

The establishment of the SHIELD Framework's six principles across two levels of assessment have been outlined to highlight key issues for consideration by the consortium and provide a framework for the legal, ethical and societal impact assessment. This report provided a legal analysis of these distinct yet interconnected settings.

This deliverable constitutes a reference document for all partners on the applicable legal, ethical and regulatory framework considerating both Union and national legislation, including EU fundamental rights and primary law, secondary EU law, and the national law of EU Member States.

Particularly, the GDPR, the LED, the ER were analysed alongside the relevant fundamental rights provisions of the CFR. Special focus was paid to the relevant terminology and principles of data protection legislation.

The aim of this report is twofold. Firstly, to establish the framework in which the capabilities can be developed in the project and on the other hand already give a first outlook in which framework INFINITY can be used operationally. The initial societal impact has also been examined, focusing primarily but not exclusively on data protection issues. In its entirety, D2.3 can be viewed as a reference document for the legal issues and societal impact as connected to the processes which will take place both within the INFINITY project and outside the project upon the completion and subsequent application of the INFINITY solution.

8 ANNEXES

8.1 ANNEX 1 QUESTIONNAIRE

LEGAL FRAMEWORK

Item no.	Question	Answer
1.*	**Directive 2016/680**: This Directive lays down the rules relating to 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, including the safeguarding against and the prevention of threats to public security. As with every EU directive, EU member states need to transpose Directive 2016/680 into national law. Please name national transposition law(s) and (if possible) provide us with a translation?	
2.*	**Directive 2016/680:** For the purposes of Directive 2016/680, do you have a specific definition for the term 'competent authority' under national law? What (national) institutions fall under the scope of the definition? Particular consideration should be given to the following roles and organisations: criminal courts, public prosecutor's office, tax authorities responsible for criminal offences, security authorities (i.e. security police), sentence enforcement authorities, and any other relevant organisations.	
3.*	**Directive 2016/680:** Under the Directive processing of personal data is "lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law." In Austria the following national laws may serve as a legal basis for processing of personal data: Security Police Act (Sicherheitspolizeigesetz), Police State Protection Act (Polizeiliches Staatsschutzgesetz), Police Cooperation Act (Polizeikooperationsgesetz) and Act on competences of armed forces (Militärbefugnisgesetz). Please list the laws of you institution's home member state that may serve as a legal basis for processing of personal data under Directive 2016/680.	

* Only to be answered by the LEA partners
* Only to be answered by the LEA partners
* Only to be answered by the LEA partners

4.	**GDPR**: Article 89 provides information on national implementation of opening clause regarding the processing of personal data for scientific research purposes. If the national implementation of this provision is relevant for the work in the INFINITY project, then can you provide a translation?	
5.	**National Legislation**: Are there national regulations on retention of data or bulk data collection (for law enforcement or scientific research purposes)? Please consult your organisation's DPO if necessary.	
6.	Is it okay for UNIVIE to directly contact your organisation's legal department and/or DPO and/or Privacy department if clarification is needed? Can you please provide the contact details of your legal department and/or DPO and/or Privacy Department?	[Please complete here] Point of Contact (I) [Please complete here] Full Name: [Please complete here] Email: [Please complete here] Tel.: [Please complete here] Point of Contact (II) [Please complete here] Full Name: [Please complete here] Email: [Please complete here] Tel.: [Please complete here] Point of Contact (III) [Please complete here] Full Name: [Please complete here] Email: [Please complete here] Tel.: [Please complete here]

9 REFERENCES

(1) *Andrew D. Selbst*, 'Disparate Impact in Big Data Policing' [2017] 52 Georgia Law Review 109-195.

(2) ALLEA - All European Academies, The European Code of Research Integrity (2017), to be found here: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf (accessed 23.08.2020).

(3) *Article 29 Data Protection Working Party*, Guidelines on consent under Regulation 2016/679 (as last revised and adopted on 10 April 2018).

(4) *Article 29 Data Protection Working Party*, Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, (as last revised and adopted 4 October 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

(5) *Article 29 Data Protection Working Party*, Opinion on some key issues of the Law Enforcement Directive 2016/680 (adopted on November 2017).

(6) *Article 29 Data Protection Working Party,* Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, WP251rev.01, As last Revised and Adopted on 6. February 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (accessed 23.11.2020).

(7) *AI HLEG*, Ethics Guidelines for Trustworthy AI, to be found here: https://ec.europa.eu/futurium/en/ai-alliance-consultation (accessed 27.08.2020).

(8) *Brayne*, 'Big Data Surveillance: The Case of Policing' [2017] 8(5) American Sociological Review 977-1008.

(9) *Brownsword, R., & Harel, A*. (2019). *Law, liberty and technology: Criminal justice in the context of smart machines*. International Journal of Law in Context, 15(2).

(10) *Biasiotti M. A.* and others, Introduction: Opportunities and Challenges for Electronic Evidence. in Maria Angela Biassiotti and others (ed), *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018).

(11) *Cavoukian*, Privacy by Design: The 7 Roundational Principles, to be found here: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (accessed 08.09.2020).

(12) *CIPL*, Artificial Intelligence and Data protection: How the GDPR regulates AI (2020) (available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf (accessed 01.02.2021).

(13) CJEU judgement of 19 September 2016 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779.

(14) CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems,Case C-311/18 *Schrems II* [2020] ECLI:EU:C:2020:559.

(15) *Cockton, G*. (2006). Designing Worth is Worth Designing. *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles.*

(16) *Craig/de Búrca*, EU Law[6] (2015).

(17) Document 32016L0680: National transposition measures communicated by the Member States concerning: 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 (EUR-Lex), https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0680 (accessed 09.11.2020).

(18) 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.

(19) *Duquenoy P*. and others, Addressing Ethical Challenges of Creating New Technology for Criminal Investigation: The VALCRI Project. in Georgios Leventakis and MR Haberfeld (eds), Societal Implications of Community-Oriented Policing and Technology (Springer Open 2018).

(20) *European Commission,* adequacy decisions https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 10.02.2020).

(21) *EC*, Ethics and Data Protecition, to be found here: https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection.pdf (accessed 08.09.2020).

(22) *EC,* Ethics in Social Science and Humanities (2018) https://ec.europa.eu/info/sites/info/files/6._h2020_ethics-soc-science-humanities_en.pdf (accessed 03.02.2021).

(23) *EC*, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020).

(24) *EDPB,* EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (revised on 30.04.2020), to be found here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (accessed 13.09.2020).

(25) *EDPB*, 'EDPB guidelines 07/2020 on the concepts of controller and processor in the GDPR' Version 1.0 (adopted on 02.09.2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (accessed 13.01.2020).

(26) *EDPB,* EDPB recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (adopted on 10.11.2020), to be found here: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (accessed 11.01.2021).

(27) *EDPB*, Response to an MEPs letter on unfair algorithms, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf (accessed 17.02.2021).

(28) *EDPS* Flowcharts and Checklists on Data Protection, to be found here: https://edps.europa.eu/sites/edp/files/publication/flowcharts_and_checklists_on_data_protection_brochure_en_1.pdf (accessed 07.09.2020).

(29) *ENISA*, Data Pseudonymisation: Advanced Techniques and Use Cases https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/ (accessed 04.02.2020).

(30) *European Data Protection Supervisor*, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (EDPS, 7 November 2019) https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf (accessed 05.09.2020).

(31) *European Data Protection Supervisor*, 'EDPS Opinion on the European commission's White Paper on Artificial Intelligence – A European approach to excellence and trust' (29 June 2020) https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf (accessed 19.02.2021).

(32) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.pdf (accessed 01.01.2021).

(33) *FRA*, Facial recognition technology: fundamental rights considerations in the context of law enforcement (2019) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (accessed 22.11.2020).

(34) *Friedman, B., Kahn, P. H. Jr., Borning, A., & Huldtgren, A.* (2013), Value sensitive design and information systems in *N. Doorn, D. Schuurbiers & I. van de Poel, M. E. Gorman (*Eds.), Early engagement and new technologies: Opening up the laboratory (Dordrecht: Springer) pp. 55–95.

(35) *Geiger* in *Geiger/Khan/Kotzur*, European Union Treaties Art 6 TEU (2015).

(36) *ICO*, overview of the principles of data protection, to be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (accessed 07.09.2020).

(37) INFINITY Grant Agreement (883293).

(38) *Jo Goodey*, 'Migration, crime and victimhood: Responses to sex trafficking in the EU' [2003] 5(4) Punishment & Society 415-431

(39) *Joh EE* (2015) The new surveillance discretion: automated suspicion, big data, and policing. Research Paper No. 473, *UC Davis Legal Studies Research Paper Series*, December.

(40) *Kroener, I., Barnard-Wills, D., & Muraszkiewicz, J.* (2019), Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems (Ethics and Information Technology) page 1–12.

(41) *Kurzweil, R*. (1999) *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*. New York: Viking.

(42) *La Fors, et al.* (2019). Reassessing values for emerging big data technologies: integrating design-based and application-based approaches. *Ethics and Information Technology*, 21(3), 209–227.

(43) *M. Flanagan and H. Nissenbaum* (2014), Values at Play in Digital Games. Cambridge, MA: MIT Press.

(44) *Nadezhda Purtova*, 'Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships ' [2018] 8(1) International Data Privacy Law 52-68.

(45) *Pozen E. D.,* The Mosaic Theory, National Security, and the Freedom of Information Act (2005) The Yale Law Journal 115:3, Dec 2005, pp. 628-679. Available at: https://www.yalelawjournal.org/note/the-mosaictheory-national-security-and-the-freedom-of-information-act.

(46) 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).

(47) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

(48) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/936/JHA and 2009/968/JHA.

(49) Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC Text with EEA relevance.

(50) *Sayers* in *Peera/Hervey/Kenner*, The EU-Charter of fundamental rights (2014).

(51) *Steneck, N.H. (*2006). Fostering integrity in research: Definitions, current knowledge, and future directions. *SCI ENG ETHICS* 12, 53–74.

(52) *Steusloff, H*. (2016). Humans Are Back in the Loop! Would Production Process Related Ethics Support the Design, Operating, and Standardization of Safe, Secure, and Efficient Human-Machine Collaboration? *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 348–350.

(53) *Tamò-Larrieux, A.* (2018). *Designing for Privacy and its Legal Framework Data Protection by Design and Default for the Internet of Things* (First edition.) Cham: Springer International Publishing.

(54) Thomson Reuters, Expert Q&A: European Data Protection Supervisor on Digital Ethics, to be found here: https://edps.europa.eu/sites/edp/files/publication/19-03-25_reuters_interview_en.pdf (accessed 20.08.2020).

(55) *Vested-Hansen* in *Peera/Hervey/Kenner*, The EU-Charter of fundamental rights (2014).

(56) Zhang T and Dong H (2008) 'Human-centred design: an emergent conceptual model', Include2009, Royal College of Art, April 8-10, 2009, *London Include2009 proceedings.*