D9.1: Research Ethics and Privacy Management

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274

Protection of Critical Infrastructures from advanced combined cyber and physical threats

Deliverable nº:	D9.1
Deliverable name:	Research Ethics and Privacy Management
Version:	1.0
Release date:	31/01/2022
Type* - Dissemination level**	Report - Public
Status:	Final
Editors	KUL
Contributing WP	WP9

Abstract

This deliverable is the outcome of the research as it is defined in the first task of WP9. More precisely, D9.1 – Research Ethics and Privacy Management represents the analysis of the relevant legal and ethical frameworks applicable to PRAETORIAN. The main aim of this deliverable is to provide general guidance on the relevant principles of data protection and research ethics related to the pilots. This includes the identification of a need to conduct a data protection impact assessment concerning the research activities, as provided by the GDPR.

Type. Report; Demonstrator; Ethics Dissemination Level. Public; Confidential (Confidential, only for members of the consortium (including the Commission Services)); RESTREINT UE (Classified information, RESTREINT UE (Commission Decision 2015/444/EC)).*

Disclaimer

PRAETORIAN

PRAETORIAN aims to enable the security stakeholders of the CIs in Europe to manage the lifecycle of security threats, from the forecast, assessment and prevention to detection, response and mitigation, in a collaborative manner with the security teams from related CIs – being the CIs in the same sector or not. The strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project will provide a multidimensional (i.e., economic, technological, policy, societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which will include digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

The project will specifically tackle (i.e., prevent, detect, respond and, in case of a declared attack, mitigate) human-made cyber and physical attacks or natural disasters affecting CIs. It will also address how an attack or incident in a specific CI can jeopardise the regular operation of other neighbouring/interrelated CIs and how to make all of them more resilient by predicting cascading effects and proposing a unified response among CIs assisting First Responder teams.

The PRAETORIAN project will test and demonstrate its results in three complementary and cross-site demonstrators organised by three international pilots, involving cross-border use cases (i.e., Spain, France and Croatia) through nine outstanding critical infrastructures: two international airports, two ports, three hospitals and two power plants. The pilot sites will interact with each other, providing feedback and lessons learnt from one demo site into the others.

The PRAETORIAN project has been financed by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101021274 on the topic of Critical Infrastructure Protection.

Document history:

Version	Date of issue	Content and changes	Partner
0.1	20.12.2021	Table of Contents	KUL
0.2	20.12.2021.	First draft	KUL
0.3	11.01.2022	Continuous input	KUL
0.4	13.01.2022	Final draft for review	KUL
1.0	27.01.2022	Final version after review	KUL

List of Authors:

Partner	Author
KUL	Halid Kayhan
KUL	Maja Nisevic
KUL	Maria Avramidou
KUL	Anton Vedder

Peer reviewed by:

Partner	**Reviewer**
ETRA	Eva Muñoz
DLR	Tim Stelkens-Kobsch
DLR	Nils Carstengerdes
EDF	Frédéric Guyomard

Table of Contents

Abbreviations and Acronyms

CFREU	Charter of Fundamental Rights of the European Union
CI	Critical Infrastructure
CETS No. 223	Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
CCTV cameras	Closed-circuit television cameras
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
GDPR	General Data Protection Regulation
H2020	Horizon 2020. The EU Framework Programme for Research and Innovation
ICT	Information and communication technologies
OECD	Organisation for Economic Co-operation and Development
EEA	European Economic Area
WP	Work Package
POPD	Protection of Personal Data
PSO	Project Security Officer
SAB	Security Advisory Board

Executive Summary

Deliverable D9.1 – Research Ethics and Privacy Management- provides a general overview of the legal and ethical requirements to be respected throughout the entire duration of the PRAETORIAN project (M1-M24). Notably, this deliverable focuses on the ethics-related aspects of the project and, specifically, on the ethical issues stemming from the involvement of human participants in PRAETORIAN, which most notably consist of the possible processing of personal data, including special categories of personal data. The ethics issues herein discussed are complemented by a set of proposed measures to mitigate the risks associated with such issues. The main aim of this deliverable is to guide the development of an ethically and legally compliant PRAETORIAN technology.

Although this deliverable provides a comprehensive legal and ethical framework, it will be further complemented by deliverable D9.2 – Legal and Ethical Frameworks and Requirements- that will produce the PRAETORIAN project's specific ethical and legal requirements.

1. Introduction

1.1 Purpose of the document

This deliverable D9.1 – Research Ethics and Privacy Management- represent the first report from the WP9 in the PRAETORIAN project. Therefore, it aims to cover a wide spectrum of ethics and privacy domains that are applicable to the research activities of the project, and in that sense, to the consortium. As indicated in the title of this report, D9.1 – Research Ethics and Privacy Management has the objective of providing guidelines on the relevant principles of data protection and research ethics related to the research activities, most notable pilots of the project. More precisely, the primary goal of the deliverable is to map the relevant domains and sources and summarise the ethical and privacy constraints and obligations, and in that sense, to outline the requirements applicable to the PRAETORIAN project. Overall, the guidance provided by this deliverable will be crucial throughout the project lifetime for the consortium to make a legally and ethically compliant research.

1.2 Scope of the document

With regard to the domains and technologies involved, this deliverable aims to be as broad as possible, thus encompassing also technologies that might possibly, but need not definitely, be applied in the PRAETORIAN project.

Ethics often constitute the basis of legislation and regulations and can also be used as an important tool to understand the rationale behind or to interpret the positive law. Therefore, ethics, to a certain degree, overlaps with law. In addition, ethics can provide guidance where the law has not still adapted completely to a new phenomenon, such as the cases of practices enabled by the technology but not anticipated by the legislator. From the PRAETORIAN project perspective, ethical issues should be seen in two main groups: the issues that may be related to the technology to be developed within the two-year project lifetime and the issues that may be relevant to the research activities leading up to the above-mentioned technology. In that sense, deliverable 9.1 focuses on the ethical issues related to the research activities during the PRAETORIAN project.

It is worth noting that this deliverable does not represent the overview of the country-by-country legal analysis. Consequently, the analysis of the specific issues regarding national level would need to

be analysed and addressed by members of the consortium or other stakeholders, in a case where the regulation of the relevant domains and questions is reserved for individual countries (e.g., when directives are left to be transposed by the Member States or where legal acts leave a broad margin of discretion to the Member States or treaty signatories).

Finally, it is important to note that while this deliverable provides a first overview of a wide spectrum of ethics and privacy domains, it also provides the basis for subsequent deliverables and work in the PRAETORIAN project.

1.3 Structure of the document

This document is structured as follows:

- Section 2 provides an overview of ethical issues relevant to the technology research methods in the PRAETORIAN project.
- Section 3 includes a brief overview of the involvement of human participants as an ethical issue identified in the Ethics- Self Assessment.
- Section 4 stresses the research on the issue around data protection as an important ethical issue, including a brief overview of the legal framework applicable to data protection.
- Section 5 focuses on the societal impact of the PRAETORIAN project, considering that it will meet the need of society because the proposed end-product of the PRAETORIAN project will increase the effectiveness of processes in the field of safetyand security reducing crime and terror threads and achieving readiness and quick response to threatening or arising emergencies.
- Section 6 mentions the dual use as an ethical issue in brief.
- Section 7 describes misuse briefly since it is one of the ethical issues identified in the Ethics-Self Assessment.
- Annex A contains the questionnaire on processing personal data in PRAETORIAN.

2. Research Ethics

As it is mentioned in Section 1, the ***ethical issues*** at stake in the PRAETORIAN project are twofold: they may be ***concerned with the technology to be developed***, but they may also be ***concerned with the research leading up to the technology itself***.

The assessment of ethical issues arising from the technology complements the codified positive legal rules and standards and looks beyond them by relying on the common moral and ethical values, such as respect for persons and their individual autonomy and freedom, the principle of justice and principle of non-maleficence, that lie at the basis of large parts of the legal systems of the European Union (EU) member states. Compliance with the highest ethical standards is essential for research excellence and the European Union, within Horizon 2020 framework, requires ethics to be an integral part of research throughout the project lifetime.[1]

The research activities during the entire lifetime of the project, in particular the testing, validation, and demonstration must comply with legal and ethical principles in order to ensure that no individual's interest or right is harmed or infringed, and public interests are not put at risk.

2.1 Research ethics in the PRAETORIAN project

At the outset, the PRAETORIAN consortium is aware that it must carry out its research and actions in compliance with ethical principles, including the highest standards of research integrity as set out, for instance, in the European Code of Conduct for Research Integrity guidelines.[2]

In addition, it must respect the ethical and legal principles and fundamental rights constituted in the Charter of Fundamental Rights of the European Union (CFREU) and the European Convention on Human Rights (ECHR) and all other applicable international, EU and national legislation. This should be demonstrated through the project's entire lifespan through careful planning and instructions, checklists, guidance, and review.

The PRAETORIAN consortium should always uphold the highest ethical standards for research, as delineated in the European Code of Conduct for Research Integrity of ALLEA (All European Academies), which was published in 2011 jointly with the ESF (European Science Foundation). According to this Code of Conduct:

[1] See European Commission, "Ethics", *Horizon2020*, last accessed on 10 January 2022.
[2] See ALLEA, *The European Code of Conduct for Research Integrity*, Revised Edition, 2017, last accessed on 10 January 2022.

> *"Good research practices are based on fundamental principles of research integrity. They guide researchers in their work as well as in their engagement with the practical, ethical and intellectual challenges inherent in research. These principles are: 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, full 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."*

To fulfil these commitments, WP9 ("Ethical, legal & societal issues") has been devoted to analyse and define best practices and recommendations, as well as to monitor project activities and report adherence, deviations and adopted countermeasures. Consequently, besides the Task T9.1- Research Ethics and Privacy Management, PRAETORIAN will assess the project's result from an ethical perspective in T9.2- Legal and Ethical Frameworks and Requirements.

In the following sections, the ethical issues identified in the Ethics-Self Assessment is examined in detail, namely:

- Involvement of human participants
- Protection of personal data
- Societal impact
- Dual use
- Misuse

As committed by the consortium members in the Grant Agreement, all the ethical issues must be addressed with the utmost respect to fundamental rights and legal standards, as recognized at the EU level, international and national levels, including but not limited to:

- Charter of Fundamental Rights of the EU (2007/C 303/01), repealing older version 2000/C 364/01
- EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), repealing Directive 95/46/EC

- Regulation on Privacy and Electronic Communications (ePrivacy Regulation), repealing Directive 2002/58/EC[3]
- Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted on 28 January 1997, as well as the modernised "Convention 108 +" (April 2019)
- Copyright Directive (Directive EU 2019/790) of 17 April 2019 on copyright and related rights in the Digital Single Market, amending Directives 96/9/EC and 2001/29/EC.
- Directive on security of network and information systems (NIS Directive) (Directive (EU) 2016/1148) concerning measures for a high common level of security of network and information systems across the Union
- Cybersecurity Act (Regulation (EU) 2019/881) of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, repealing Regulation (EU) No 526/2013
- Rome Declaration on Responsible Research and Innovation in Europe, 21 November 2014

Lastly, the consortium has established an Ethics Board in order to address the issues related to ethics and data protection in the best possible way. The Ethics Board membership, composed by independent members with relevant experience in the field, has been reported at M3 in Deliverable D11.6: GEN- Requirement No.6. The Board has an objective of monitoring ethics issues in the project and how they are handled and for this purpose, they will issue two reports: one at M12 (D11.7: GEN-Requirement No. 7) and the second one at M24 (D11.8: GEN- Requirement No.8).

[3] The ePrivacy Regulation 2021 is a draft regulation from the EU Council that governs all electronic communications on publicly available services and networks from individuals inside the European Union. The EU's data privacy regime currently consists of the GDPR and the ePrivacy Directive from 2002. The new ePrivacy Regulation would repeal and replace the older 2002 directive (also known as the EU cookie law) and bring significant updates by including new technologies in its legal framework.

3. Involvement of Human Participants as ethical issue

The Ethics Self-Assessment, as a part of the Grant Agreement, states that PRAETORIAN will involve human beings on a voluntary and responsible basis (i.e., consent-based and free of charge) taking part inhe pilots, as well as other stakeholders involved as external experts or taking as part of project events. This section will provide ethical guidance regarding involvement of human participations in the light of the European Commission's Guidelines on Ethics-Self Assessment for Horizon2020 Projects[4] as well as the above-mentioned Ethics Self-Assessment of the PRAETORIAN project.

The consortium must conduct its research based on the following basic ethical rules:

- **Respect for persons**: research will aim to maximize the benefit for individuals and society and minimize risk and harm; the rights, dignity, health, non-discrimination, non-malevolence and well-being of individuals and groups will be respected.
- **Voluntary and appropriately informed participation**: the involved participants will be adults voluntarily engaged, based on direct negotiation on the set-up of the research and the potential risk of being harmed in any way. Their consent to participate will be given freely and based on an understanding of the risks and benefits. The project will avoid invading privacy, maintain the confidentiality of data, obtain informed consent and remain available for the whole process for providing any necessary information. Protocols and documents will be implemented and translated into local languages.
- **Gender balance**: a gender policy will be followed to guarantee gender balance during the overall project, according to the research process for Horizon 2020. Two are the main pillars of such a gender policy: i) to seek gender balance in the composition of research teams, groups of volunteers involved in field studies, project workshops and consultations with experts; ii) to ensure gender balance in decision making.
- **Responsible conduct of research**: the consortium will carry both ethical and regulatory responsibilities to protect the welfare and interests of individuals, to design the study so as to minimize risks to them, and to obtain adequate training for protecting their interests and welfare. The research will be conducted with integrity, transparency and independence

[4] European Commission Directorate-General for Research & Innovation, "*Horizon 2020 Programme Guidance: How to complete your ethics self-assessment*", Version 6.1, 4 February 2019.

avoiding conflicts of interest, while lines of responsibility and accountability will be clearly defined.

- **Mutual duty of care**: all research partners will have a mutual duty of care to each other to maintain the project's autonomy. They will also have a duty of care to participants in ensuring that they are not put at risk of harm, as a result of their participation.

It is also committed that ethical ground rules will apply to ancillary staff, including data collectors, secretarial staff, and others, such as interpreters. They should be informed of the strict confidentiality requirements and the need to respect the principle of non-disclosure. Whenever human beings are involved in the project, information on privacy and confidentiality, and the evidence about the compliance with national and EU legislation should be provided to project participants.

The participation of vulnerable individuals or groups and persons unable to give valid consent (e.g., children/minors, persons judged as lacking sufficient mental capacity, elderly, etc) will be avoided. If patient data collection and processing is necessary to fulfil the project objectives, this should be carefully assessed during the project and reported.

PRAETORIAN should develop a procedure for the identification and recruitment of research participants, taking into account these groups of individuals by implementing risk-mitigation measures. This will be reported as part of D11.1: H- Requirement No. 1. This deliverable will also provide informed consent procedures, as well as templates.

It is crucial that participants in the research carried out within PRAETORIAN are involved in a **voluntary way**, free from any coercion or risk. This requires to avoid risks of **undue inducement**. Therefore, monetary compensation for participation should be avoided. Nonetheless, forms of in-kind compensation to participants for the time they have dedicated to the project can be considered (for instance, education on the GDPR or other regulations, or certain aspects of the technology to be developed in detail etc.).

To ensure voluntary nature of participation, potential research participants must be informed about the project, its purpose, methods and intended possible uses, but also about what their participation in the research entails and what risks are involved. This information must be provided to them in an **accessible format**.

Informed consent is key in research ethics to ensure voluntary participation in research. It is important to clarify that there are **two types of informed consent** in such research projects:

i. informed consent as ethical standard in research;

ii. informed consent as a principle of data protection.

The existence of these two co-existing forms of consent, and their intertwined relationship, is often not completely clear nor very straightforward. As acknowledged by the European Data Protection Supervisor (EDPS), in its Preliminary Opinion on data protection and scientific research, *"there is some (understandable) confusion regarding consent, which is a principle of both data protection and research involving human participants"*.

In certain types of research, these two "layers" of consent are (more clearly) distinct. However, in a research project like PRAETORIAN, consent as a principle of research ethics and consent as a principle of data protection tend to somehow overlap since the involvement of human participants in the research activities equates to the processing of personal data.

In PRAETORIAN, whenever human participants are involved, they will be thoroughly informed through an information sheet and informed consent form. The information sheets and consent forms should:

- be written in clear and plain language and in terms fully understandable to the participants in order to enable participants to exercise their rights;
- describe the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomforts that might be involved;
- underline that participation is voluntary and that anyone has the right to refuse to participate and to withdraw at any time without giving a reason and without any disadvantage;
- describe the purpose of data processing and the duration of retention;
- provide information regarding the legal rights of the participants to access, correct, block or delete their data, including right to not be subject of automated decision- making process or profiling;
- specify the personal data to be collected, and to what degree confidentiality of such data will be ensured; and
- inform to the participants about who will be in charge of storing the collected data and who will have access to those data.

Participants must consent in writing to participate in the research, by signing the information sheet and informed consent form. The informed consent procedures, as well as the templates (in languages and terms eligible for participants), will be reported in D11.1: H- Requirement No. 1.

An appropriate **recruitment strategy** should be adopted for the participants. While preparing it, possible authoritative or hierarchical positions with respect to the participants (e.g., participant's supervisor or employer) should be taken into account. As noted previously, D11.1: H- Requirement No. 1 will include this strategy.

European Commission highlights that the general principle is to maximize benefits and minimize risks/harms from the ethics perspective in H2020 research projects involving human participants[5]. For this reason, the PRAETORIAN consortium should ensure that the risks and harms to the participants are minimized and benefits are maximized. This requires the consortium members to assume the task of making efforts to guarantee respect for people and human dignity, fair distribution of research benefits and burden of research, and protecting the values, rights, and interest of the research participants.

Furthermore, the applicable law of the pilot countries should be taken duly into account and appropriate measures should be implemented in order to ensure that the rights and freedoms of the participants are always safeguarded. Deliverable D11.3: POPD- Requirement No. 3 has already provided the current overview of the technical and organizational measures that will be implemented to safeguard the rights and freedoms of the data subjects' participants. Deliverable D11.2: H- Requirement No.2 will also provide copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans (Information Sheets and Consent Forms).

, As reported in D11.3: POPD- Requirement No. 3, some of the consortium partners (i.e. UPV, SDMIS, IDEMIA, HEP, DLR, and THALES) have appointed a DPO that oversees the collection and processing of personal data in the context of their research activities. These DPO take also responsibility for the PRAETORIAN project. In that sense, the data subjects will be able to exercise their rights by contacting the relevant partners' DPO, and the contact details of DPO should be made available to all data subjects involved in the research.

[5] European Commission Directorate-General for Research & Innovation, "*Horizon 2020 Programme Guidance: How to complete your ethics self-assessment*", Version 6.1, 4 February 2019, last accessed on 10 January 2022, p.8.

4. Data protection as ethical issue

It is worth noting that there is a significant overlap with this deliverable (particularly this section) and the already submitted Deliverable 11.3. This D11.3 is a part of WP11- Ethics requirements, which is aimed at ensuring compliance with the Ethics requirements set out by the European Commission (EC). It has already presented a description of the concept of 'personal data' and subsequently provides an overview of the relevant EU and international frameworks that apply to the processing of personal data, such as the fundamental right to data protection and the GDPR. In addition, it has the objective of providing details on key aspects relating to the processing of personal data, such as the data minimization approach and accompanying technical, organizational, and security measures in the context of the research activities of PRAETORIAN, in accordance with POPD- Requirement No. 3. D11.3 has provided a first preliminary overview of the information that will be further updated in upcoming Ethics deliverables as well as the PRAETORIAN data protection policy, to be published in M14 together with the update of the Data Management Plan (D1.4v2).

This above-mentioned D11.3 describes, among other topics, what personal data are supposed to be processed in PRAETORIAN, how this personal data is limited and necessary for the research objectives, and what technical, organizational, and security measures are supposed to be implemented to safeguard the rights and freedoms of data subjects in PRAETORIAN. This means that:

- all data collected is restricted to what is strictly needed by the project following standards driven by those operators in terms of security and confidentiality, most notably reducing the number of data subjects participating in the research activities as low as is necessary,
- the consortium will define technical and organizational measures to safeguard the rights and freedoms of the research participants (i.e., data subjects),
- security measures aim to comprise physical and logical access control of personal data,
- personal data will be stored securely and, if necessary, will be de-identified through anonymization or a pseudo-anonymizing code, including the erasure or fully and irreversibly anonymization of personal data after the storage period has elapsed,
- consortium partners will also make use of end-to-end encryption to securely transfer data when requested to handle EU classified information that may be generated in the project,
- the technical, organizational, and security measures will address the data protection of personal data during video collection and analysis, as detecting and tracking individuals from the collected video footage is one of the research objectives of the PRAETORIAN project,

- where personal data is processed – the project will obtain a free and informed consent of the data subjects, whose personal data will be processed,
- where personal data is processed, this shall only be done for the specific purposes to which data subjects have given their informed consent,
- where personal data is processed, it will not be kept for longer than is absolutely necessary for the purposes of each processing activity,
- where human participation should occur in the project – the project will obtain a written informed (explicit) consent of the subjects to participate.

It must be noted that D11.3 was a preliminary overview of the key aspects related to the processing of personal data based on the information provided by relevant consortium partners through a questionnaire. This questionnaire is shared as the annex of this deliverable D9.1. Due to the maturity of the project and the fact that some of the necessary information was not yet known, it was not feasible to provide a complete and accurate overview in D11.3. In order to provide more accurate and complete information, including a detailed overview of personal data processing activities, technical and organizational measures, security measures, and the exercise of data subject rights, additional information is required from different WPs. This includes, among other topics, additional information regarding the pilot demonstrations and the integration and verification plan (D7.1 'Integration and verification plan' - M11). The Ethics Board meeting with the corresponding Ethics Board report due in M12 can also provide additional insights into the ethical risks concerning personal data processing in PRAETORIAN, particularly relating to the pilot demonstrations. This additional information and feedback will be incorporated in the future Ethics deliverables as well as the PRAETORIAN data protection policy, to be published in M14 together with the update of the Data Management Plan (D1.4v2).

D11.3 has also provided the consortium partners with a brief overview of relevant EU and international legislation relating to the processing of personal data and has provided the EC with a first preliminary overview of key aspects relating to the processing of personal data.

Considering this overlap and the content of the deliverable that has already been provided in the D11.3, this section of the current deliverable will refrain from unnecessary repetitions (unless it is essential to provide a comprehensive and complete framework) and will not go into the details if those aspects have already been covered by D11.3.

4.1 Personal Data Protection

As outlined by the D11.3, it is crucial to provide definitions of the concepts of personal data processing and personal data. According to the EU GDPR ***personal data processing*** covers the 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 of personal data. Furthermore, the GDPR applies to the processing of personal data wholly or partly by automated means and non-automated processing if it is part of a structured filing system. Hence, any novel and innovative technical tools for collecting and processing data of individuals must be designed with their interests and based on European values, fundamental rights and rules.

The definition of ***personal data*** is 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. Despite this definition adopted by the GDPR, there is no normative guidance on applying this concept to particular technology or systems. Nevertheless, a general analysis of the elements of the definition following the work of the Article 29 Working Party opinion could help with classifying certain types of data as 'personal' concerning the PRAETORIAN project.[6]

As the D11.3 has already clarified, the notion of personal data defined as any information relating to an identified or identifiable natural person indicates that the information is personal not only when an immediate inference can be made using direct identifiers such as a name, fingerprints, or biometric data, but also when intermediate measures can be taken to connect that piece of information to an individual. Besides, if identifying a data subject takes a disproportionate amount of time, cost, or human resources, the probability of identification seems to be negligible in reality.

It should, further be noted that some personal data are particularly sensitive as they reveal information that could pose a significant risk to individuals' fundamental rights and freedoms.[7]

[6] See Art. 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20 June 2007.

[7] The GDPR defines sensitive data as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely

Therefore, misuse or mishandling of these data can facilitate human rights abuses or unfair discrimination. Since the GDPR accepts a risk-based approach, sensitive data receive special status and higher protection in the GDPR. In a sense, the GDPR prohibits processing these categories of data unless certain conditions are met.[8]

4.2 Legal Frameworks Related to Personal Data Protection

D11.3 has already outlined the most prominent legal texts, when it comes to the fundamental rights and data protection. These are *theECHR*[9] in the context of the Council of Europe and *the CFREU*[10] in the context of the European Union. Both the ECHR and the CFREU are of primary importance for the EU Member States.

In the context of the PRAETORIAN project, the ECHR is relevant since it guarantees the right to respect for one's private and family life, home, and correspondence under Article 8. The right to data protection, albeit not explicitly referred in Article 8 ECHR, forms part of the rights protected under this Article. As such, it creates obligations to protect against arbitrary interferences with private and family life, home, and correspondence. Since personal data processing is an example of such interferences, PRAETORIAN shall fully comply with the ECHR.

CFREU is also relevant, *in the context of the PRAETORIAN project*, because of the data processing concerning the purpose of the project. Different from the ECHR which does not include an explicit reference to right to data protection but still protects it under the right to respect for private and family life, the CFREU specifies that personal data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access data collected concerning him or her and the right to have it rectified. Thus, the CFREU has introduced a right to protection of personal data (Article 8), separate from the right to respect for private and family life (Article 7).

In addition, a range of other legal frameworks is of major importance for data protection. Analytically, the *GDPR,* which was adopted by the European Union in May 2016, is a landmark in the

---

identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation." See Article 9 (1) GDPR.

[8] Article 9 (2) GDPR.

[9] See European Convention on Human Rights - Official texts, Convention and Protocols (coe.int), (last accessed on 5 November, 2021).

[10] See EU Charter of Fundamental Rights | European Commission (europa.eu), (last accessed on 5 November 5, 2021).

EU's data protection law as it exercised influence around the world and set the global standard for data protection legislation. The GDPR entered into force on 25 May 2018 and replaced the Data Protection Directive (Directive 95/46/EC; DPD). The GDPR is the principal EU legal instrument regulating data protection at the EU level.

As explained by the D11.3, the GDPR lays down rules relating to the protection of natural persons concerning the processing of their personal data and rules relating to the free movement of personal data. The rules cover the processing of personal data wholly or partly by automated means and the manual processing of personal data if that data form part or are intended to form part of a filing system. These rules cover both the public and private sectors but do not cover the processing of personal data by EU institutions, bodies, offices and agencies. Processing personal data for purely personal and household activities are also exempted from the scope of the GDPR. When the processing of personal data is done for national security reasons or prevention, investigation, detection or prosecution of criminal offences, including the safeguarding of public security, the GDPR rules do not apply. The GDPR applies to the European Economic Area (EEA), which includes all EU Member states and Liechtenstein, Iceland, and Norway. The GDPR applies to the personal data processing in the context of activities of a controller or a processor based in the EU, without importance where the actual processing takes place.[11] The GDPR also applies to a controller or a processor based outside of the EU if they process personal data of individuals in the EU in the context of offering goods or services or monitoring the individuals' behaviours within the EU.

The GDPR applies to PRAETORIAN and will be at the core of this section since, as noted above, it is the principal EU level legal instrument for personal data protection. To ensure GDPR compliance, it is critical to correctly identify the controller(s) and processor(s), including the type of data that are going to be processed in the PRAETORIAN ecosystem.

It is important to further note that the Council of Europe Convention 108[12] and Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[13] seems to be relevant as well for PRAETORIAN.

---

[11] According to the GDPR, **Data Controller –** Is a legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it (Article 4 (7) GDPR), and **Data Processor –** Is a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of a data controller (Article 4 (8) GDPR).
[12] See Convention 108 and Protocols (coe.int), (last accessed on November 5, 2021).
[13] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD, (last accessed on November 5, 2021).

The *Convention 108* was the first legally binding international instrument that dealt with data protection. In 2001, an Additional Protocol to Convention 108 was adopted. It introduced provisions on data flows to third countries and on the mandatory establishment of independent national data protection supervisory authorities. In 2018, Convention 108 underwent a modernisation process that culminated in adopting Protocol CETS No. 223. This modernisation process had two main objectives: to deal with the challenges of using information and communication technologies (ICT); and to make the implementation of Convention 108 more effective. *In the context of the PRAETORIAN project,* Convention 108 may be relevant since the Contracting States of the Convention 108 are required to take the necessary steps in their domestic legislation to apply the principles it lays down. Therefore, the Convention 108 provides a benchmark for PRAETORIAN to understand the fundamental rights that all individuals from the Contracting States enjoy concerning the processing of personal data. It is worth clarifying that the content of the Convention 108 is in line with the GDPR and there is no need for an extra assessment as long as the principles and obligations under the GDPR are fulfilled.

The *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal* were adopted in 1980 by the OECD. The primary aim of the OECD guidelines is to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. These guidelines, which contained the first internationally agreed-upon set of privacy principles, have influenced legislation and policy in OECD member countries and beyond. *In the context of the PRAETORIAN project*, it should be clarified that OECD guidelines are not legally binding. However, the OECD guidelines play an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. Demonstrating compliance with the OECD privacy principles seems reasonable in promoting respect and preservation of privacy when it comes to PRAETORIAN. However, as it is the case with Convention 108, there is no need to make a detailed assessment regarding OECD guidelines since they are also in line with the GDPR. The fact that the underlying principles of these different documents are the same or highly similar shows how important it is to comply with them.

Lastly, in addition to the above-mentioned legal frameworks, there are also national legal frameworks for data protection. These frameworks must be in line with the GDPR (since it is a Regulation) but may also contain special derogations (national implementations of the GDPR might differ on some aspects since the GDPR leaves room for Member State discretion in terms of implementation).

4.3 Data Protection Principles

Based on the responses provided by the PRAETORIAN consortium partners to the questionnaire that is shared in the Annex A of this deliverable, the D11.3 has noted that although there are partners that intend not to use personal data in the algorithms and tools developed, the purpose of the PRAETORIAN project at some parts requires the processing of personal data. In a sense, the objective of the PRAETORIAN project follows the needs for collecting and processing personal data such as, for instance, first names, surnames, e-mail addresses, phone numbers, occupation, video data, and location. The mentioned types of personal data will be collected from surveys and/or interviews. Thus, the GDPR must be fully complied with by the project partners.

The GDPR principles underlying the processing of personal data can also be found in the Convention 108 and the OECD guidelines.[14] As regards the processing of personal data, the principles enshrined in the Convention 108 concern in particular the lawful and fair collection and processing of personal data, for specified legitimate purposes. This entails the requirement for compliance with the principles as lawfulness, fairness and transparency, purpose limitation, storage limitation, quality assurance including data accuracy, as well as data security. In a similar manner, the OECD guidelines stipulate the importance of the principles of data minimisation, data quality, purpose limitation, transparency (''openness'') and accountability. It is **important to highlight that since the GDPR is the primary binding legal document in all the EU member states with regards to the protection of personal data, the analysis of legal requirements will be based on this regulation in this sub-section as well as the next ones.**

The principles of data protection enshrined in the GDPR must be applied throughout the lifetime of the project, to ensure that all the ethical issues arising from the processing activity, which take place within the project, are tackled properly.

Art. 5 GDPR stipulates that the processing of personal data must be compliant with the following principles:

- lawfulness, fairness and transparency;
- purpose limitation;

[14] See Convention 108 and Protocols (coe.int), (last accessed on 12 January, 2022) and OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD, (last accessed on 12 January, 2022).

- data minimisation;
- data accuracy;
- storage limitation;
- integrity and confidentiality.

These principles are explained in the table below:

Principle of processing	***Importance for the PRAETORIAN***
Lawfulness (Art. 5(1)(a) GDPR)	The principle of lawfulness requires personal data to be processed only if and to the extent that the processing activity can be based on one of the legal bases listed under Art. 6 GDPR (or under Art. 9 GDPR in the case of special categories of data). As mentioned earlier, the processing of the special categories of data identified under Art. 9(1) GDPR is in principle prohibited, except where the lawful basis for processing is to be found in Art. 6 in combination with one of the exceptions listed under Art. 9(2) GDPR. Any processing of personal data needs to be preceded by a careful and thorough assessment of the legal basis on which such processing can be grounded.
Fairness (Art. 5(1)(a) GDPR)	As required by the principle of fairness, controllers must inform the data subjects that the processing will be performed in accordance with the principles of lawfulness and transparency. Furthermore, processing operations must not be performed in secret and the data subject must be informed

	about the possible risks that may be caused by the processing.[15]
Transparency (Art. 5(1)(a) GDPR)	According to the principle of transparency, the data subjects must be informed about how their data are processed and about their rights as data subjects. Such information must be given to the data subjects prior to the processing and must remain available and accessible to them in the course of the processing (including on the occasion of an access request).[16] In a research project like PRAETORIAN, the participants/data subjects should be made aware of all the relevant information regarding the processing of their personal data in the context of the research. Information sheets and informed consent forms must ensure that data subjects are properly informed and that the research does not take place "in secret". In addition to the pilots, this principle should also be implemented and respected in the course of any activities related to the project website.
Purpose limitation (Art. 5(1)(b) GDPR)	For each processing activity, there must be a specified, explicit and legitimate purpose, which must be determined prior to the processing. Any processing for undefined purposes, as well as any further processing that is incompatible with the original one, is unlawful. Art. 5(1)(b) GDPR introduces a presumption of compatibility, which is subject to the requirements under Art. 89 GDPR, for further processing for archiving purposes in the public interest,

[15] EU Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Luxembourg, Publications Office of the European Union, 2018, Section 3.1.2.
[16] ibid, p. 120.

	scientific or historical research purposes or statistical purposes. From the outset to the end of the project, PRAETORIAN project partners should avoid further processing for purposes that are not compatible with the purpose of conducting this scientific research.
Data minimisation (Art. 5(1) (c) GDPR)	The data minimisation principle requires limiting the processing of personal data, as long as these are adequate and relevant, to what is necessary to achieve the purposes for which they are processed. The PRAETORIAN consortium is required to take the necessary measures to ensure only the strictly necessary data is collected and processed. It is important to highlight that the D11.3 has already noted, based on the partners' responses to the annexed questionnaire, that all data collected has been restricted to what was strictly needed by the project following standards driven by those operators in terms of security and confidentiality, most notably reducing the number of data subjects participating in the research activities as low as is necessary.
Data accuracy (Art. 5(1) (d) GDPR)	The data accuracy principle requires ensuring the accuracy of the data collected and processed and, where necessary, keeping it up to date. For this reason, every reasonable step must be taken to ensure that personal data that are inaccurate, for the purposes for which they are processed, are erased or rectified without delay. Thus, data need to be checked regularly and kept up to date in order to secure accuracy by the PRAETORIAN partners, while

	inaccurate data need to be erased or rectified without delay.
Storage limitation (Art. 5(1)(e) GDPR)	Where personal data is processed, it must be kept only as long as it is necessary for the project purposes to be achieved.
Data security (Art. 5(1)(f) GDPR)	A combination of technical and organizational measures, which must be appropriate to prevent the risk of unauthorized or unlawful processing and accidental loss, destruction or damage must be taken to achieve integrity and confidentiality of the data. The PRAETORIAN consortium is required to ensure that state-of-the-art technical and organizational measures are implemented from the outset until the end of the project. According to art. 25 GDPR, the principles of data protection by design and by default also need to be implemented throughout the project. In line with these principles, measures on, among others, access-control shall be taken to prevent unauthorised persons from gaining access to data per se or data processing systems. In other words, it shall be ensured that persons authorised to access personal data and use data processing systems have access only to those data that they are authorised to access, and that personal data cannot be read, copied, altered or removed without authorisation during processing. Personal data will be pseudonymised and, where feasible, anonymised. The partners should also consider the possibility of processing the data on-premises, i.e., on servers accessible only locally to prevent any connection from outside. Overall, partners must ensure that personal data are kept securely (Art. 32 GDPR), and that publication does not breach

	confidentiality or anonymity.
Accountability (Art. 5(2) GDPR)	According to the principle of accountability, controllers and processors are required to implement the technical and organizational measures to comply - and to be able to demonstrate compliance - with data processing obligations. This deliverable maps the legal and ethical framework that contributes to helping the consortium to fulfil the obligations deriving from the accountability principle. Thus, this can be regarded as an important step to demonstrate compliance with the legal and technical requirements set by the legislation. The consortium must also consider promoting compliance with the accountability by adopting certain measures including: • records of processing activities • data protection by design and by default • a data protection impact assessment (DPIA) specifically for types of processing that are likely to result in a high risk to the rights and freedoms of the data subjects in accordance with the GDPR – for instance, in the case of automated decision-making.

In line with the principle of accountability of the GDPR, when the research involves processing of personal data, H2020 ethics guidelines[17] require providing certain information as follows:

a) Details of the technical and organisational measures to safeguard the rights of the research participants. – For instance: For organisations that must appoint a DPO under the GDPR:

[17] European Commission Directorate-General for Research & Innovation, "*Horizon 2020 Programme Guidance: How to complete your ethics self-assessment*", Version 6.1, 4 February 2019, accessed 04 June 2021, p. 17.

Involvement of the DPO and disclosure of the contact details to the research participants. For all other organisations: Details of the data protection policy for the project (i.e., project-specific, not general).

b) Details of the informed consent procedures.

c) Details of the security measures to prevent unauthorised access to personal data.

d) How all the processed data is relevant and limited to the purposes of the project (”data minimisation” principle).

e) Details of the anonymisation/pseudonymisation techniques.

f) Justification of why research data will not be anonymised/pseudonymised (if relevant).

g) Details of the data transfers (type of data transferred and country to which it is transferred – for both EU and non-EU countries).

Furthermore, H2020 ethics guidelines also require, if relevant, informed consent forms and information sheets used to be provided/kept in the file.

Besides all the above, it is also important to consider that national laws can also play an important role in connection with the pilots that will be carried out in different countries. National legislation must be carefully assessed, in particular to identify the requirements under Art. 89(1) GDPR, which are applicable to the further processing of data for research purposes.

4.3.1 Lawfulness of the processing of personal data

As required by the principle of lawfulness, an appropriate legal basis, under Art. 6 GDPR (and under Art. 9(2) GDPR in the case of special categories of data) must be identified prior to any personal data processing activity.

Before each processing activity, a **case-by-case assessment** of the most appropriate legal basis must be performed. The appropriate legal basis needs to be analysed for both the primary processing of personal data (when the partners collect data from participants and undertake any initial processing activity) and the secondary processing (processing of data for a purpose other than the one for which the data was initially collected).

Under Art. 6 (1) GDPR, the possible legal bases are:

a) data subject's consent

b) performance of a contract to which the data subject is party or, in order to take steps at the request of the data subject, prior to entering into a contract

c) compliance with a legal obligation to which the controller is subject

d) vital interests of the data subject or of another natural person

e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

f) legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

As noted above, a case-by-case assessment needs to be done by the data controller prior to each processing activity.

4.3.1.1 Informed Consent

If data subjects' consent is the applicable legal basis for the data processing as a part of PRAETORIAN research activities, that must be informed. In other words, consent can only be a legal basis if data subjects are properly informed about the processing activity and the risks that may involve. It is important to note that, this informed consent is different from the one related to research ethics. This issue has already been explained in detail under Section 3: Involvement of Human Participants.

This informed consent form, which will be provided by the relevant partners to the human participants, must take into consideration the following requirements:

- written in clear and plain language (in terms completely understandable to the participants)
- describing the aims, methods and implications of the research and the data processing activities envisaged within the research, and any benefits, risks or discomforts that might be involved

- explicitly stating that participation and being subject to data processing is voluntary and that everyone has the right to refuse to participate and to withdraw at any time without giving a reason and without any disadvantage

- detailing the purpose of data processing and duration of retention

- detailing the legal rights of the participants to access, correct, block or delete their data

- specifying the personal data that will be collected, and to what degree (and how) confidentiality of such data will be ensured

- providing information to the participants concerning who will be in charge of storing the collected data and who will have access to those data.

4.3.2 Lawfulness of further processing for scientific research purposes

Under Art. 5(1)(b) GDPR which regulates the principle of purpose limitation, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. However, "presumption of compatibility", as aforementioned, is introduced by the same article for the further processing of personal data for scientific research purposes when such further processing is in compliance with Art. 89(1) GDPR.

The presumption of compatibility requires the adoption of appropriate technical and organizational measures aimed at ensuring data minimization (Art. 89(1) GDPR). It can be achieved, particularly, through measures such as pseudonymization, access limitation or even anonymization, in cases where the same purposes can be achieved with anonymised data.

On the condition that these technical and organizational measures are implemented, the processing of personal data for scientific research purposes can take place in derogation of certain data subject rights (access, rectification, restriction of processing, object), where the EU or Member State law allows for such derogations (Art. 89(2) GDPR). Hence, it is always imperative to also investigate the applicable national laws in the context of research.

However, the EDPS has warned that the presumption of compatibility cannot be interpreted as a general authorisation for further processing of personal data for scientific purposes: "Each case must be considered on its own merits and circumstances. But in principle, personal data collected in the

commercial or healthcare context, for example, may be further used for scientific research purposes, by the original or a new controller, if appropriate safeguards are in place".[18]

Regarding the principle of lawfulness (and the need to identify a specific legal basis prior to any processing activity), Recital 50 GDPR that is non-binding , states that in case of personal data being processed for secondary compatible purposes, "no legal basis separate from that which allowed the collection of the personal data is required. […] Further processing for […] scientific research purposes shall be considered to be compatible lawful processing operations". The Recital seems to address both personal and special categories of data since it is not accompanied by prescriptive legal provisions in the GDPR.

Although the principles of purpose limitation and lawfulness seem to overlap, the EDPS argues that "in order to ensure respect for the rights of the data subject, the compatibility test under Art. 6(4) should still be considered prior to the re-use of data for the purposes of scientific research, particularly where the data was originally collected for very different purposes or outside the area of scientific research".[19]

Art. 6(4) provides that "Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law", the compatibility of the further processing must be assessed on the basis of:

a) the link between the initial purpose of collection and the secondary purpose;

b) the context of collection of the data, with a particular attention to the relationship between the data subject and the controller;

c) the nature of the personal data, in particular whether special categories of data or data related to criminal conviction or offences are processed;

d) the possible consequences of the further processing for data subjects;

e) the existence of appropriate safeguards such as pseudonymization or encryption.

[18] EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, 6 January 2020, accessed 04 June 2021, Section 6.7.
[19] ibid.

Furthermore, where research partners would further process previously collected personal data, e.g., pre-existing data sets or sources, partners will follow the H2020 ethics guidelines[20]. In parallel with the above-mentioned GDPR provision, the partners shall be able to provide adequate information concerning

a) Details of the database used or of the source of the data

b) Details of the data processing operations

c) How the rights of the research participants will be safeguarded

d) How all the processed data is relevant and limited to the purposes of the project ("data minimisation"principle)

e) Where relevant, why the research data will not be anonymised/pseudonymised

In addition, the following documents will be provided/kept on file:

a) a declaration wherein the lawful basis for the data processing is explicitly confirmed

b) if applicable, the permission by the owner/manager of the data sets

c) informed consent forms and information sheets where applicable

In light of all the above, national laws governing research activities will have to be analysed and applied, together with the provision referred above, to the specific case, particularly within the pilots.

The D11.3 has already noted that in addition to obtaining new informed valid consent from data subjects concerning further personal data processing as required by the GDPR, the partners also commit to securely transferring the previously collected data by using end-to-end encryption or ZIP-file encryption, including file and password access policies, access rights restrictions, and logs to ensure that only authorised personnel can access the personal data.

[20] European Commission Directorate-General for Research & Innovation, "*Horizon 2020 Programme Guidance: How to complete your ethics self-assessment*", Version 6.1, 4 February 2019, accessed 04 June 2021, p. 18.

4.4 Data Subjects Rights

The data subject, the natural person whose personal data is being collected and processed, is granted certain rights under the Chapter III of GDPR. These rights are important as they will result in certain obligations for data controllers and data processors. Data subjects have certain rights as listed below:

1) right to be informed about any processing of their personal data
2) right to access their own personal data and obtain information about the processing
3) right to the rectification of their personal data, so that these are accurate and up to date
4) right to the erasure of their personal data (right to be forgotten), under certain conditions
5) right to temporarily restrict the processing of their data
6) right to data portability, meaning to transfer their data from one controller to another, under certain conditions
7) right to object to the processing of their data, under certain conditions
8) right not to be subject to solely automated decision-making, under certain conditions along with other rights relevant to automated decision-making

The project must take the necessary measures to ensure data subjects to be able to practice their rights. Exemptions may apply in certain cases, as will be explained in the next deliverable of WP9, the deliverable 9.2.

4.5 International Data Transfers

In the EU context, the GDPR contains specific rules for the transfers of personal data from the EU to third countries or international organisations. Precisely, under the Chapter V of the GDPR, transfers of personal data from the EU to third countries or international organisations are defined as international data transfers. Since all the partners involved in the PRAETORIAN project are based in the EU, this chapter of the GDPR does not seem to be of high importance during the research activities. However, in case an international data transfer may be considered for any reason, the explanations provided below must be taken into due account. For instance, this may be the case if a

cloud system or cloud-based software offered by a service provider based in the US is used by the project partners to collect, store or process personal data within the PRAETORIAN project.

According to the Chapter V of the GDPR, when data transfers need to occur from the EU to the third countries, these shall be predicated on one of the following grounds:

- an "adequacy determination" by the EC in respect of the country in question
- a data-transfer agreement containing EC standard contractual clauses giving effect to EU data protection law or
- binding corporate rules covering both sender and recipient and approved by a national supervisory authority
- the explicit consent of the data subject (which requires them to be informed in advance of any such transfers).

Additionally, H2020 ethics guidelines require to provide certain information listed below when it is planned to export data from the EU to non-EU countries:

a) details of the types of personal data to be exported

b) how the rights of the research participants will be safeguarded.

In addition, a declaration that confirms compliance with Chapter V of the GDPR needs to be provided/kept in the file.[21] On the other hand, in case of a transfer from any of these countries to the EU, the applicable law in that country will apply. According to H2020 ethics guidelines, information on details of the types of personal data to be imported shall be provided, and a declaration confirming compliance with the laws of the country in which the data was collected shall be provided/kept in the file.[22] In both cases (import and export), it is essential to specify the types of personal data and countries involved.

[21] European Commission Directorate-General for Research & Innovation, "*Horizon 2020 Programme Guidance: How to complete your ethics self-assessment*", Version 6.1, 4 February 2019, accessed 04 June 2021, p.19.
[22] ibid.

4.6 Technical, Organisational and Security Measures

The D11.3 has already stressed the need for the deployment of technical, organizational and security measures related to PRAETORIAN research activities. Based on the information provided by the partners, these measures include the safe storage of personal data and potentially anonymisation and pseudonymisation. Security measures entail that personal data should be password protected, securely stored and access to that data will be allowed solely for the purpose of the research and to the researchers employed for the PRAETORIAN project. At the same time specific technical, organizational and security measures e.g., blurring of images, in relation to video footage which is one of the research objectives of the PRAETORIAN project are proposed. Lastly, the existence of free, specific, unambiguous, and informed consent of the data subjects following the standards defined by the applicable data protection law, the ability of data subjects to withdraw such consent as well as the fact that such consent will be given in a written form are stressed.

All the necessary steps should be taken throughout the project to fulfil these commitments and any further measure should always be considered to better protect personal data.

4.7 Ethical Risks of the Personal Data Processing Activities

The D11.3 has already provided an overview of the main identified ethical risks related to the personal data processing activities during the research in PRAETORIAN. The overview is based on the information provided by the partners.

The first identified risk is the potential of unethical use of patient data, which qualifies as a special category of personal data under art. 9 of the GDPR (i.e., sensitive personal data), considering the participation of several hospitals as end users in the PRAETORIAN project.

It is important to remind that MUG, as a hospital CI operator, commits to not generating or processing personal data during the PRAETORIAN project. On the other hand, HULAFE, another hospital CI operator, in the event that non-anonymous surveys are necessary, they commit to conducting them as an end user to collect the weaknesses and strengths of the system implemented in PRAETORIAN, as well as the added value and experience of some of the operators of their critical infrastructure. If such surveys are necessary, only personal data collected via those non-anonymous surveys (without combining with any other dataset) are planned to be processed by HULAFE. The personal data of patients belonging to the hospital (i.e., sensitive personal data) will not be shared or processed in the context of PRAETORIAN, which mitigates the risk of unethical use of patient data.

Also, before any survey is conducted, an ethics committee of PRAETORIAN consortium will review both the activity and the processing of the data.

As the second major risk, the data processing activities performed in the context of video analytics for intrusion detection and threat identification, based on the advanced person and vehicle detection and tracking, may also give rise to potential ethical concerns, specifically related to the tracking and observation of individuals and the potential resulting profiling possibilities. This risk is, however, seen as mitigated by the implementation of appropriate technical, organizational, and security measures as described previously. Additionally, the technology particularly developed by the project partner IDEMIA for PRAETORIAN does not offer profiling capabilities but rather aims at automating a process (mainly intrusion detection from CCTV cameras), which otherwise could also be achieved by manual observation. Thus, it offers significant economic advantages, qualitative improvements and shorter reaction times. Finally, if necessary, IDEMIA also commits to making use of synthetically generated data in the research activities during PRAETORIAN, in order to further mitigate potential ethical concerns related to the processing of personal data of research participants.

4.8 Data Protection Impact Assessment (DPIA)

The GDPR mandates that where a processing activity is likely to pose high risks 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” (Art. 35(1) GDPR). This is called Data Protection Impact Assessment (DPIA).

Under Art. 35 (3) GDPR, a DPIA is made necessary, in particular, where the processing entails

a) a systematic and extensive evaluation of personal aspects based on automated decision making, including profiling,

b) processing on a large scale of special categories of data or

c) a systematic monitoring of a publicly accessible area on a large scale.

However, this is not an exhaustive list and data processing activities not included in this list that incurs a high risk for the rights and freedoms of natural persons will still be subject to a DPIA. Taking

this non-exhaustive nature into account, Article 29 Working Party has also published a set of criteria to identify the need to conduct a DPIA in different scenarios.[23]

The D11.3 has already provided a comprehensive overview with regards to data protection impact assessments and for this reason, the repetitions are avoided here. Project partners should refer to that deliverable for further information.

Since it is not covered by the D11.3, it should be noted here that the H2020 ethics guidelines[24] stipulate that when data processing "involve profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as, tracking, surveillance, audio and video recording, geolocation tracking etc.) or any other data processing operation that may result in a high risk to the rights and freedoms of the research participants", certain information shall be provided:

a) Details of the methods used for tracking, surveillance or observation of participants.

b) Details of the methods used for profiling.

c) Risk assessment for the data processing activities.

d) How harm will be prevented, and the rights of the research participants safeguarded.

e) Details on the procedures for informing the research participants about profiling, and its possible consequences and the protection measures.

Furthermore, according to H2020 ethics guidelines[25], if relevant, an opinion of the data controller on the need for a data protection impact assessment shall also be provided/kept in the file.

Lastly, it is worth reminding that the D11.3 has already provided an opinion on whether a DPIA is required to be carried out for the PRAETORIAN research project as follows: Considering the current information and plans regarding the processing of personal data in PRAETORIAN (based on the partners' responses to the questionnaire), while taking into account the criteria established by art. 35 GDPR and Article 29 Working Party, a DPIA is not needed *per se* for the PRAETORIAN research

[23] Art. 29 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, WP 248 rev. 01, adopted on 04 April 2017, as last revised and adopted on 04 October 2017.
[24] ibid., p. 18.
[25] ibid., p. 18.

activities. However, it is important to distinguish the need to conduct a DPIA for the PRAETORIAN research activities from a DPIA for the end use of the PRAETORIAN tools and solutions in a real-world scenario. In the latter case, it is highly probable that several of the criteria may be met, for example, the prediction of the movements and location of data subjects, the systemic and large-scale monitoring of data subjects, and the systemic and large-scale processing of special categories of personal data. Consequently, the obligation to conduct a DPIA falls under the responsibility of the data controller in such an end-use scenario.

4.9 National Derogations to Certain GDPR Provisions

The D11.3 has already provided an overview of the derogations to **the processing of biometric data** and **data subject rights** found in the national laws of Germany, Spain, France and Croatia. For the sake of brevity, they are not repeated in this current deliverable and the consortium partners conducting research activities in these Member States should refer to that deliverable. Those partners must take into account their respective national data protection legislation and the accompanying derogations found therein, as explained in the D11.3.

5. Societal Impact

One of the issues touched upon in the Ethics-Self Assessment was societal impacts of the PRAETORIAN project considering that it will meet the need of society. This is because the proposed end-product of the PRAETORIAN project will increase the effectiveness of processes in the field of safety, reducing crime and terror threats and achieving readiness and quick response to threatening or arising emergencies. This can potentially have an impact particularly on the EU citizens living in the cities.

For this reason, the potential societal trade-offs associated with the implementation of the different proposed measures will be taken into account throughout the WP9 ("Ethical, legal & regulatory issues"), thus in this deliverable as well as the upcoming ones.

The issues identified, related to societal impact, in the Ethics-Self Assessment, as well as key points to take into account, are listed below:

- The proposed research will address documented societal security need(s) (e.g., life, liberty, health, employment, property, environment, values).
    - One of the objectives of the PRAETORIAN project is to address society's security needs of respect for private life and data protection in a safer environment. Respect for private life and data protection are both enshrined in the EU Charter of Fundamental Rights. On the other hand, the GDPR further strengthens individuals' rights, giving them better control of their data and ensuring that their privacy continues to be protected in the digital age. To achieve this objective, PRAETORIAN aims to innovate functionalities and services for protecting people, offering complementary services that will greatly enhance citizens' data protection and improve the physical and cybersecurity of cities.
- The research output will meet these needs, this will be demonstrated and the level of societal acceptance will be assessed.
    - The PRAETORIAN project aims at improving the coordination among the public and private security operators to build up a safe environment for citizens where respect for their private life is guaranteed. These aspects will be demonstrated through full-

scale evaluation activities that will be conducted during the project lifetime in collaboration with final users. The effectiveness of the PRAETORIAN approach will be demonstrated in 4 pilot sites in 3 different EU member states.

- Furthermore, to avoid problems arising from emerging technologies that could have an impact from the societal point of view, final users are foreseen to be involved not only in the evaluation of the PRAETORIAN technological products but also in their designs. From the citizens' perspective, the project dissemination activities, which are carried out by WP10, aim at communicating and explaining the characteristics of the PRAETORIAN products and their added value, together with the societal impact assessment. These dissemination activities will also be used to collect feedback and data on citizens' feelings and perceptions about security and the impact of emerging technologies on them.

- The research will address threats to society (e.g., crime, terrorism, pandemic, natural and manmade disasters etc.).

  - An essential part of what the PRAETORIAN project is willing to achieve is to increase the effectiveness of processes in the field of safety and safeguard cities and individuals from potential natural and man-made disasters, crime and terror threats, as well as data and privacy infringement.

- The proposed research will address in an appropriate way the above-mentioned threats.

  - PRAETORIAN takes an innovative approach to answer appropriately to the above-mentioned challenges by developing a common cybersecurity framework and customized technologies enabling CI to:

    1) secure access protocols to existing and future smart systems, and therefore improving security, privacy and data protection risks;

    2) model and analyse real and potential incidents and test the interactions between different security actors, thus improving awareness of vulnerabilities, attacks and risks that influence life and business of CI;

3) improve their strategic, operative and tactic capabilities by dynamically aggregating and processing large and heterogeneous amounts of data, and offering an advanced Hybrid Situational Awareness interface;

4) enhance adoption and better address CI's changing needs, by using standard and well-known industry standards and common practices for design and implementation of the technologies;

5) give fast and effective support in their operative action;

6) exploit cross-sectoral synergies and co-define mitigation strategies by engaging smart city stakeholders' collaboration.

- The research will benefit society.
    - Certain segments of society will benefit from the proposed research since beneficiaries of the work conducted in this project are those stakeholders directly affected by the threats that will be addressed by this research. Those beneficiaries are, including but not limited to, critical infrastructures (ports, airports, hospitals, powerplants among others), public transportations, malls, and other crowded areas as well as individuals, whose security and privacy needs to be protected.
    - On the other hand, society as a whole will also benefit from the research because the PRAETORIAN project aims to foster the confidence of data subjects in ICT technologies and the Digital Single Market, contributing to new business ideas, stimulating the EU economy, technological development and the general level of data security. Thus, the project has the potential to foster progress and economic growth and to increase the sense of justice and security, consequently impacting also social wellbeing.
- The research will not have any negative impact on society.
    - It is not foreseen that the research could have a negative impact on the rights and values enshrined in the treaties (e.g. freedom of association, freedom of expression, protection of personal dignity, privacy and data protection), or it could impact disproportionately upon specific groups or unduly discriminate against them. On the

contrary, the PRAETORIAN is committed to upholding European values. For this reason, it will be based on the concept of monitoring and securing personal data processing. Thus, organizations using the PRAETORIAN end-products will be able to provide transparency and accountability and this will contribute to better data governance and to a higher trust of citizens in those organizations.

As mentioned above, these explanations are based on the commitments made by the PRAETORIAN consortium in the Ethics Self-Assessment. It is clear that all the necessary actions should be taken to fulfil these commitments and the priority should always be to protect society while providing the greatest benefit and avoiding any possible harm. Furthermore, European values enshrined in the European treaties as well as the legislations, including but not limited to the EU Charter of Fundamental Rights and the GDPR, must always be upheld throughout the project. All these were taken into account while preparing this deliverable (and will also be the case for the next WP9 deliverables) and the project partners must be well aware of all these explanations and principles.

6. Dual Use as ethical issue

At the international and EU level, the legislator has set up a regulatory regime to control the export of "dual-use" items. The term '"dual-use" refers to items, including software and technology, that can be used for both civil applications and military purposes. In this context, deliverable D11.4 as part of WP11- Ethics requirements aims to ensure compliance with the Ethics requirements set out by the European Commission.

The main objective of deliverable D11.4 was to provide details on potential dual-use implications and risk-mitigation strategies of the project, according to DU- Requirement No. 4. Therefore, D11.4 provides a general overview of control regimes for dual-use items and describes the relevant international and EU legal framework. Most notably, this deliverable provides an overview of the Wassenaar Arrangement and EU Regulation 2021/821 that are applicable to dual-use items. In addition, deliverable D11.4 further explains the EU framework and important dual-use concepts, definitions, and responsibilities, including explanations which categories on the list of dual-use items may be relevant for the technologies used and developed in PRAETORIAN. Deliverable D11.4 also includes identification and description of several risks related to dual-use items, including to inform PRAETORIAN partners about potential ***'exports'***, which can occur inadvertently through Intangible Technology Transfers, and their qualification as ***'exporters'***. Following deliverable D11.4, PRAETORIAN partners must obtain the appropriate approval prior to any exports to comply with the dual-use controls regime. This is accompanied by an obligation to exercise due diligence regarding potential dual-use risks and implications of the used and developed technologies. In order to adequately address any dual-use risks and implications, a dual-use risk monitoring & management strategy will be developed and kept up to date.

Since D11.4 identifies some of the risks, in the end, it formulates several recommendations and measures that PRAETORIAN partners should consider in the course of the project.

Deliverable D11.4 classified the risks to ***non-compliance risks***, including the consequent investigations and convictions, criminal litigation proceedings, financial sanctions and revocation of authorisations, and ***reputational risks,*** *which* can also be relevant, including exposure in case of unlawful exports, complaints and hacktivism against exporters. In this context, deliverable D11.4 identified recommendations and measures, such obtaining the relevant authorisations and licencing either with the form of a Union General Export Authorisation or a National Export Authorisation (general, individual or global) depending on the specific context. Furthermore, partners should respect the limits of the authorisations granted and perform their accountability-related obligations

through record-keeping and registry mechanisms. At the same time, partners should adopt measures to prevent, mitigate, and monitor dual-use risks and corrective measures when required.

7. Misuse as ethical issue

One of the potential ethical risks involves the ***misuse of research findings*****,** such as research data, methods, knowledge, or developed technologies.

Following the EC guidelines, the potential misuse of research may be defined as "*research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes".*[26]

The issue of misuse of research findings was the subject matter of the deliverable D11.5, as a part of WP11- Ethics requirements. Deliverable D11.5 aims at ensuring compliance with the Ethics requirements set out by the European Commission in the context of misuse of research findings. Therefore, deliverable D11.5 represents a specific deliverable that had the objective of providing details on potential misuse implications. In this context, deliverable D11.5 explains the concept of misuse of research findings and gives information on identifying and addressing the potential misuse of research findings based on the existing EC guidelines. In addition, it includes a brief project overview and zooms in on the general and specific PRAETORIAN research aspects that may be relevant for the potential misuse of research findings. Finally, deliverable D11.5 gives an overview of recommendations and measures to prevent, mitigate, and correct potential risks of misuse.

It is good to note that the concept of misuse is not a part of a strict legal framework. Instead, the EC has issued several documents that serve as guidelines to identify and address risks of potential misuse of research findings.

In order to identify and address risks of potential misuse of research findings in PRAETORIAN, a questionnaire has been developed that has been circulated among all PRAETORIAN partners. In addition, the approach adopted in the questionnaire was based on the EC guidelines on potential misuse of research. Based on the questionnaires, deliverable D11.5 concludes as follows:

- The PRAETORIAN research can be considered to provide knowledge, materials, and technologies that could be channelled into crime or terrorism. Specifically, the research findings (e.g., vulnerability and risk assessments), if they ended up in the wrong hands, could lead to physical or cyber-attacks on CIs by exploiting the identified weaknesses,

[26] European Commission, *Guidance note – Potential misuse of research*, Version 1.1, 07 January 2020, last accessed 10 January 2022, p.1.

- The PRAETORIAN research also involves technologies that can be used for surveillance purposes with the potential to curtail human rights and civil liberties. This applies to the video analytics software for physical intrusion detection and threat identification in particular, for which surveillance is the intended and lawful purpose,

- It is doubtful that the PRAETORIAN research could result in chemical, biological, radiological or nuclear weapons or the means for their delivery,

- PRAETORIAN does not involve minorities or vulnerable groups and does not develop social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

Since deliverable D11.5 discovered either general or specific risks for PRAETORIAN, in order to address these risks of potential misuse, the PRAETORIAN consortium and its partners have implemented several measures to prevent, mitigate, and correct risks of misuse. These measures include, among others, the appointment of a SAB and PSO and an Ethics Board to oversee the handling of sensitive information and address potential ethical issues. Multiple deliverables have also been made consortium confidential (limited dissemination, CO) or classified as RESTREINT UE/EU RESTRICTED to protect and secure sensitive information that may be misused. Partners involved in vulnerable research areas, i.e., IDEMIA, will also use synthetically generated 3D data to mitigate risks of potential misuse further. Finally, a PRAETORIAN misuse risk monitoring and management strategy will be developed and kept up to date.

8. Conclusions

Within the framework of the EU's Horizon2020 Research and Innovation Programme, ethics is required to be an integral part of the PREATORIAN project from the outset until the end of the project. Compliance with the highest ethical standards is essential for research excellence.

The assessment of ethical issues arising from the technology, in addition to the legal and regulatory framework, allows to go beyond those frameworks by relying on the common moral and ethical values, such as respect for persons and their individual autonomy and freedom, the principle of justice and principle of non-maleficence, that lie at the basis of large parts of the legal systems of the EU member states. Thus, in each step of the project and in particular during the testing and validation, the project must comply with legal and ethical principles in order to ensure that no individual's interest or right is harmed or infringed, and public interests are not put at risk.

This current deliverable, Deliverable D9.1-Research Ethics and Privacy Management provides a general overview of the legal and ethical requirements to be respected throughout the entire lifetime of the PRAETORIAN project (M1-M24) in order to guide the development of an ethically and legally compliant PRAETORIAN technology. Notably, this deliverable focuses on the ethics-related aspects of the project and, specifically, on the ethical issues stemming from the involvement of human participants in PRAETORIAN, which most notably consist of the possible processing of personal data, including special categories of data. The explanations of these ethics' issues are complemented by the applicable frameworks as well as a set of proposed measures to mitigate the risks associated with those issues.

The framework provided by this deliverable (D9.1) will be complemented by Deliverable D9.2 "Legal and Ethical Frameworks and Requirements" that will be based on the PRAETORIAN project's specific ethical and legal requirements. D9.2 will provide an overview of EU legislation on privacy and data protection, cybersecurity, and CIs (e.g., the NIS Directive, GDPR, CI framework, etc.). Particular attention will be given to the balancing of rights and interests, more specifically the rights of individuals (e.g., the right to privacy and data protection) and society (e.g., the protection of CIs). To highlight the difference between the two, the current deliverable, D9.1, provides a legal and ethical framework applicable, primarily, to PRAETORIAN research activities, while the D9.2 has the aim of providing the necessary framework for the technology to be developed.

9. References

ALLEA, *The European Code of Conduct for Research Integrity*, Revised Edition, 2017, last accessed on 10 January 2022.

Article 29 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, WP 248 rev. 01, adopted on 4 April 2017, as last revised and adopted on 4 October 2017.

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20th June 2007.

Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981.

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950.

EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, 6 January 2020, last accessed 4 June 2021.

EU Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Luxembourg, Publications Office of the European Union, 2018.

European Commission, "Ethics", *Horizon2020*, last accessed on 10 January 2022.

European Commission, *Guidance note – Potential misuse of research*, Version 1.1, 7 January 2020, last accessed 10 January 2022.

European Commission Directorate-General for Research & Innovation, "*Horizon 2020 Programme Guidance: How to complete your ethics self-assessment*", Version 6.1, 4 February 2019.

European Union: Council of the European Union, *Charter of Fundamental Rights of the European Union (2007/C 303/01)*, 14 December 2007, C 303/1.

Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980.

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.

Annexes

I. ANNEX A: Questionnaire on processing of personal data in PRAETORIAN

Which personal data will be processed during the research of the project? *See above for the definition of 'personal data'. Note that if the data has been made irreversibly anonymous, it no longer qualifies as 'personal data'*	*For example: collection and processing of first names, surnames, e-mail addresses, occupation, and age in the context of research activities XYZ in pilot case X (e.g., surveys, interviews, user testing, etc.) amongst a sample of CI operators.*
Explain why this data is **relevant and limited to the purposes** of the research project	*For examples: collection and processing of the personal data is necessary in the context of surveys and/or interviews amongst a sample of CI operators in order to identify security problems, needs, and expectations. The names and e-mail addresses are necessary to contact and inform the participants. The occupation and age are necessary because of reasons XYZ.*
Describe the **technical and organizational measures** that will be implemented to safeguard the rights and freedoms of the data subjects/research participants	*For example: personal data will be securely stored and pseudonymized using XYZ encryption techniques. Our organization has appointed a DPO that oversees the collection and processing of personal data in the context of the research activities. Data subjects are able to exercise their data subject rights (e.g., right to withdraw consent, right to object, right of erasure, etc.) by contacting our organization's Data Protection Officer (DPO) or the PRAETORIAN DPO.*
Describe the **security**	*For example: personal data will be securely transferred using end-*

measures that will be implemented **to prevent unauthorized access** to personal data, or the equipment used for the processing	*to-end encryption. Personal data will be securely stored and pseudonymized using XYZ encryption techniques. Access policies XYZ, restrictions XYZ, and logs ensure that only authorized personnel are able to access the personal data.*
Describe the **anonymization/pseudonymisation techniques** that will be implemented	*For example: personal data will be securely transferred using end-to-end encryption and securely stored and pseudonymized using XYZ encryption techniques. Personal data will be anonymized using XYZ techniques.*
Will there be further processing of **previously collected personal data**? **If yes**, provide an explicit confirmation that the one who will be further processing has a lawful basis for the data processing and that the appropriate technical and organizational measures are in place to safeguard the rights of the data subjects	*For example: we will process personal datasets previously collected in project X or in context Y.* *For example: we rely on the original consent of the data subjects (which includes the processing for research purposes in PRAETORIAN) or we will obtain new valid consent from each data subject. Previously collected personal data will be securely transferred using end-to-end encryption and securely stored and pseudonymized using XYZ encryption techniques.*
Will personal data be exchanged among public and technical and private partners? **If yes, what kind of data** and information will be	*For example: personal data on XYZ will be exchanged among technical and private partners XYZ for the purposes of XYZ. This includes sensitive data on XYZ (e.g., biometric data) resulting from facial recognition activities. For examples relating to pseudonymization, technical & organizational measures, and security measures, see questions above.*

exchanged? **If yes**, does it include sensitive personal data, data deriving from tracking and observation of people, data resulting from face recognition activities? *See above for the definition of 'sensitive personal data'.* **If yes**, how will the data be pseudonymised? **If yes**, how will the rights of the data subjects involved be protected (e.g., technical & organizational measures, security measures, access & storage policies, etc.)?	
Do you know of any special derogations pertaining to (1) the rights of the data subjects or (2) the processing of biometric data have been established under the national legislation of the country where the research takes place? **If yes**, please submit a declaration of compliance with respective national legal framework(s).	*For example: specific data subject rights, such as the right to object and right to erasure, are subject to additional conditions XYZ under national legislation. The processing of biometric data is prohibited for purposes XYZ under national legislation.*
Only for the host institutions	

of research activities: Please provide a confirmation that you have appointed a **Data Protection Officer (DPO)** and information on the relevant competencies of the DPO Please provide the **contact details of the DPO** (which must also be made available to all data subjects involved in the research) In case you are not obliged to appoint a DPO under the GDPR, please provide a detailed data protection policy for the project	