Public

CounteR

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

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

Deliverable number 7.3

Ethics Briefing Pack 1st Version

Work Package	WP 7 Data Privacy & Ethics Requirements
Task	Task 7.3 Ethics Briefing Pack 1st Version
Lead Beneficiary	MITLA
Due Date	Month 8
Submission Date	31 January 2022
Deliverable Status	Final Version
Deliverable Type	R (Report)
Dissemination Level	Public
Document Name	D7.3 (Ethics Briefing Pack 1st Version)

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

Disclaimer

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

Editors

Surname	First Name	Beneficiary
Zammit Maempel	Michael	MITLA

Contributors

Surname	First Name	Beneficiary
Valenzia	Alexia	MITLA
Camilleri	Jake	MITLA

Reviewers

Surname	First Name	Beneficiary
Zammit Maempel	Michael	MITLA

History of Changes

Version	Date	Change	Modified by
0.1	01/12/2021	Initial Draft	Jake Camilleri
0.2	23/12/2021	Review and feedback	Dana Tantu, Catalin Trufin
0.3	23/12/2021	Implementing feedback	Jake Camilleri
0.4	17/01/2022	Quality Check	Jake Camilleri
0.5	17/01/2022	Review and Feedback	Mariano Zamorano
0.6	19/01/2022	Quality Check (II)	Alexia Valenzia, Jake Camilleri
1.0	20/01/2022	Final version	Michael Zammit Maempel

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

Table of Contents

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

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

Executive Summary

The aim of this Deliverable is specifically that of ensuring compliance by all Project partners with the legal and regulatory aspects of data privacy and protection. The process of compliance is an ongoing one, which will need to be monitored throughout the entire lifespan of the Project, and with corrective action taken as required. Given that this Deliverable is being drawn up at the initial stage of the Project at a time when actual data has not started being processed or even collected, this Deliverable proposes a pre-emptive framework for how Personal Data should be collected and processed. Once the technicalities of the Project are more clearly defined, this deliverable will be fine-tuned and built-up by D7.4 which is due in month 22.

The role of checking compliance will pass on to the Data Protection Officer of the entire Consortium as well as the individual Data Protection Officers of the partners themselves working in conjunction with each other. In providing guidance and periodic checks, this team of Data Protection Officers can best ensure that the aims of the Project are observed while respecting applicable data protection requirements. Wherever possible and in order to make the use of this Deliverable as relevant as can be, this Deliverable presents the basic legal position set out in the GDPR (EC Regulation 2016/679), which represents the starting point to be adopted by all partners when evaluating their respective compliance levels.

This document will summarise the legal requirements of the GDPR and those activities that will be expected to take place during the course of the Project in order to highlight whether data protection provisions need to be considered or not.

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

List of Abbreviations

Abbreviation	Name
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
D	Deliverable
DoA	Description of the Action
GDPR	General Data Protection Regulation (EU Regulation 2016/679)
PD	Personal Data
Project or Counter	Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection
SCPDs	Special Categories of Personal Data
WP	Work Package

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

List of Figures

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

List of Tables

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

1 Introduction

1.1 Description of task

Task 7.3 (to which this deliverable relates) is aimed at devising ethical guidelines according to any ethical issues that will have to be addressed during the Project's lifecycle. This Deliverable includes a legal and ethical analysis to be undertaken and recommendations for legal compliance during fieldwork. This first version of the CounteR research ethics briefing pack includes guidelines for research and pilots (corresponding to WP9) and highlights ethical issues related to each stage of the Project and other issues that are raised by partners during the process.

This Deliverable tries to help sustain a more critical perspective on research ethics, covering two main aspects:

a) those related to data protection and informed consent; and
b) those related to ethical research.

This document includes detailed information about informed consent and authorization for Personal Data management requirements and procedures. In this way, CounteR will guarantee respect for the ethical principles and fundamental rights embedded in the regulatory framework of the European Union.

1.2 Relation with other tasks and deliverables

Significant importance is given to data management within the CounteR work package structure (as seen in the figure below) mainly due to the value of the data and its potential for use for future research.

Figure 1 - Relationship between Working Packages

This Deliverable is part of WP7 – Data Privacy and Ethics Requirements and is directly related to both WP10 – Management and WP11 – Ethics Requirements. In particular, D7.3 is connected to:

Deliverable Number	Deliverable Title	Nature of Relation
10.3	Data Management Plan	This Deliverable is particularly relevant to Sections 2, 3, 5 and 6 of D10.3, which describe the Data Summary, Fair Data, Data Security and Ethical Aspects respectively.
11.1	H – Requirement No. 1	This Deliverable is related to D11.1 as both documents include templates of the informed consent/assent forms and information sheets.
11.2	POPD – Requirement No. 3	This Deliverable is related to D11.2 as both documents include information related to the initial Personal Datasets identified and a short description of the measures that will be employed to protect the privacy and confidentiality of the data subjects (anonymisation, pseudonymisation).

Table 1 - Relation to other Deliverables

This Deliverable is also related to:

a) WP9 *Dissemination, ecosystem development and exploitation* as it includes guidelines for research and pilots; and
b) Task 3.4 *Data Management* within WP3 as this task will have the key objective to present an in-depth and comprehensive report on the infrastructure and technology that will manage data collected.

1.3 Methodology

The DoA describes this Deliverable as:

> *This task is aimed at devising ethical guidelines according to any ethical issues that will have to be addressed during the Project's lifecycle (D7.3). This Deliverable includes a legal and ethical analysis to be undertaken and recommendations will be made for legal compliance during fieldwork. CounteR research ethics briefing pack will include guidelines for research and pilots (WP9) and which will highlight ethical issues related to each stage of the Project and other issues that are raised by partners during the process. This dialogue would help to sustain a more critical perspective on research ethics, covering two main aspects: (1) those related to data protection and informed consent and (2) those related to ethical research. Also, the Consortium will receive training on how to detect and tackle privacy and ethical issues during the Project Pilots and discuss ethical aspects concerning the guidelines for end-users developed within WP8. This training will be conducted during a seminar to be held in Month 6. Both the outline of this session and its results will be fully explained in D7.3. This document will include detailed information about informed consent and authorization for Personal Data management requirements and procedures. In this way, CounteR will guarantee respect for the ethical principles and fundamental rights*

embedded in the regulatory framework of the EU. Concretely, in this way CounteR will ensure respect for the ethical principles and fundamental rights embedded in the regulatory framework of the European Union.

This Deliverable has been prepared using the principles concerning the protection of Personal Data as a foundation and these principles where then used when compiling the sections on ethics and risk management. The contents of D1.1, D1.2, D1.5, D11.1 and D11.2 were also reviewed when drafting this Deliverable.

1.4 Deliverable structure

This document includes the following sections:

a) Executive Summary;
b) Introduction;
c) Classification of Data Used in the Counter Project;
d) Legal Requirements
e) Technical and Organisational Measures
f) Issues regarding Consent;
g) Ethical Guidelines;
h) Data Protection Impact Assessments;
i) Conclusion; and
j) Appendices:
    i. Privacy policy;
    ii. Access policy;
    iii. Retention policy;
    iv. Privacy notice template;
    v. Informed consent template;
    vi. Data sharing agreement; and
    vii. Legitimate interest assessment template.

2 CLASSIFICATION OF DATA USED IN THE COUNTER PROJECT

This document will detail specific activities where data privacy regulation needs to be considered and the procedures to be followed by the Consortium in order to cover the Ethics Requirements for data privacy at the level of the Project. This document provides general Ethical Guidelines shared and approved by the entire Consortium, which will be used along the entire research path in order to effectively manage any ethical requirements and possible issues that arise related to data privacy.

There are two categories of partners in the Project that might handle Personal Data:

a) Partners that contribute to the development and validation of the CounteR solution. Such partners shall be responsible for developing the technicalities of the solution and the way in which in shall work;
b) LEA partners that will pilot and validate the CounteR solution.

ETICAS and MITLA, as legal and ethics experts, will be involved in reviewing the overall activity of the Project, and ensuring this is compliant with the fundamental rights and freedoms of individuals, and the various ethical and legal requirements that need to be observed. For this reason, they will not be processing Personal Data in any way.

Before processing Personal Data, partners may in some cases need to obtain authorisations/approvals in order to be able to perform their respective tasks that involve processing of Personal Data. In this Deliverable these details regarding the partners that require authorizations/approvals are included wherever possible.

Horizon 2020 ethics standards and rules will be implemented to the fullest extent possible, irrespectively of the country where the study is conducted. Ethics is dealt within the Horizon 2020 legislation at various levels. A specific Ethical Appraisal Procedure in Horizon 2020 Projects exists to ensure ethical compliance. The Horizon 2020 Regulation of Establishment establishes in Article 19 (Ethical principles) that: “All the research and innovation activities carried out under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of Personal Data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection.” The legal state of the art reflected in D7.1, including all relevant requirements for CounteR development, and requirements elaborated as part of WP11 will guide partners to ensure these rights. Moreover, the ethical implications of the CounteR technology design, testing and implementation thoroughly reviewed in these documents are systematized and operationalized within the present Deliverable.

The below includes various ethical requirements, which Project Partners should abide by, in order to comply with the Horizon 2020 ethical standards. *Inter alia*, this includes Regulation (EU) No. 1291/2013 of the European Parliament and of the Council of December 2013 (“**Regulation (EU) No. 1291/2013**”). As a general rule-of-thumb however, it should be noted that **consent** is the main pillar in ensuring fairness of data processing.

At the on sent, **Article 16** of the abovementioned Regulation requires any Projects funded under the Horizon-2020 programme to ensure the effective promotion of gender equality, as well as the general gender dimension within research and innovation content. In particular, attention shall be paid to ensuring gender balance, subject to the context in which the research is conducted. Such context includes: the situation in the field of research and innovation concerned, evaluation panels and bodies such as advisory groups and expert groups.

Furthermore, **Article 19** establishes certain ethical obligations which the CounteR solution must adhere to, whereby all research and innovation activities carried out under Horizon 2020 "shall comply with ethical principles and relevant national, Union and international legislation". In particular, the principles which the CounteR Project shall adhere to include the following:

1) principle of **proportionality**;
2) the right to **privacy**;
3) the right to the **protection of Personal Data**;
4) the right to the **physical** and **mental integrity of a person**;
5) the right to **non-discrimination** and the need to ensure **high levels of human health protection**;

Given the nature of the Project, certain ethical risks must be considered. A brief overview of such risks may be found in the diagram below. Note the below is to serve as guiding principles, as is not to be interpreted as an exhaustive list – for ethical concerns develop in tandem with the Project.

Ethical Risks to be Considered

Discrimination	**Stigmatisation**	**Data Misuse**
Participants	**Third Parties**	**Communities**
Data Breaches	**Data Security**	**Reputation**
Occupational risks	**Participant's wellbeing**	

Ancillary considerations which Project Partners should implement are as follows:

1) The DPO should play a key role in in ensuring compliance and safeguarding the rights of the research participants;
2) Specific derogation reminder (for health, genetic and biometric data);
3) Data minimisation principle to be adhered at all times;
4) Anonymisation pseudonymisation as a default safeguard;
5) Stringent data security measures;
6) Evaluation of the ethics risks related to the data processing activities of the Project. This includes an opinion if data protection impact assessment should be conducted under art.35 GDPR.

Furthermore, the European Commission has issues documentation (14 November 2018) which specifically concerns the interplay between ethics and data protection in research Projects such as CounteR. The most salient points of such documentation are detailed hereunder.

Pseudonymisation and Anonymisation

One of the best ways to mitigate ethical concerns arising from the use of Personal Data is to anonymise such data so that it no longer relates to an identifiable person. Data that no longer relates to identifiable persons, such as aggregate and statistical data, or data that has otherwise been rendered anonymous so that the data subject cannot be re-identified, is not Personal Data and is therefore outside the scope of data protection law.

However, even if one plans on using only anonymised datasets, the proposal may still raise significant ethics issues. These could relate to the origins of the data or the manner in which they were obtained. Project Partners must therefore specify the source of the datasets intended to be used within proposal and address any ethics issues that arise. Partners must also consider the potential for misuse of the research methodology or findings, and the risk of harm to the group or community that the data concern.

Where it is necessary to retain a link between the research subjects and their Personal Data, Project Partners should, wherever possible, pseudonymise the data in order to protect the data subject's privacy and minimise the risk to their fundamental rights in the event of unauthorised access. Pseudonymisation and anonymisation are not the same thing and it is important that Project Partners are aware of the difference between them, as the GDPR requires to use them wherever possible or feasible (Article 89 GDPR).

While anonymised data is no longer considered Personal Data, anonymisation processes are challenging, particularly where large datasets containing a wide range of Personal Data are concerned. This is because it is exceedingly difficult to create fully anonymous datasets that retain the granular information needed for research purposes. As far as CounteR is concerned, if there is a significant prospect of re-identification of persons whose data has been collected, the information should be treated as Personal Data. It is difficult to assess the risk of re-identification with absolute certainty and Project Partners should always err on the side of caution. A growing body of case studies and research publications in which individuals are identified from 'anonymous' datasets have demonstrated the fundamental constraints to anonymisation as a technique to protect the privacy of individuals.

If Project Partners intend to anonymise the data collected for use in the CounteR research Project, the timing of the anonymisation process is paramount. Project Partners are collecting 'anonymised' data only if the anonymisation happens at the point and time at which the data are collected from the research subject, so that no Personal Data are actually processed. If anonymisation takes place at a later stage, e.g., Project Partners intend to remove personally identifiable information during the transcription of audio recordings or at the point at which survey data are fed into a database, the raw data are still Personal Data and Project Partners proposal must include provisions for their protection up until the point at which they are deleted or rendered anonymous.

In certain instances, Project Partners may be required to keep the raw data for auditing, accountability or research integrity purposes. There may be other scenarios in which a host institution has a raw dataset which it makes available to its researchers and partners in anonymised form. In these instances, while the recipients of the anonymised data may – subject to the mitigation of the risk of re-identification – be exempt from data protection requirements, the host institution is still processing Personal Data and must therefore ensure appropriate protection for the raw (personal) data. This includes technical and organisational measures to protect the data and the means to identify the data subjects (e.g., the keys, codes or applications used to anonymise the data) against unauthorised access or use. If Project Partners are in any doubt as to the adequacy of the technique(s) that Project Partners intend to use, Project Partners should seek advice from their DPO or a suitably qualified expert. Sensitive or complex processing scenarios involving pseudonymisation or anonymisation, it may even be necessary to conduct a DPIA in order to ensure an appropriate level of data protection and minimise risk to the data subjects' rights.

Data Protection by Design and Default

To innovate ethically and responsibly, researchers and developers have long been encouraged to apply the concept of 'privacy by design,' which provides a framework for focusing the design of systems, databases and processes on respect for data subjects' fundamental rights. A wider concept of 'data protection by design,' now included in the GDPR, requires data controllers to implement appropriate technical and organisational measures to give effect to the GDPR's core data-protection principles (articles 5 and 25 GDPR). Data protection by design is one of the best ways to address the ethics concerns that arise from Project Partners research proposal at the design stage of the Project

In a research and development context, measures to achieve data protection by design could include:

- the pseudonymisation or anonymisation of Personal Data;
- data minimisation;
- applied cryptography (e.g., encryption and hashing);
- using data-protection focused service providers and storage platforms; and
- arrangements that enable data subjects to exercise their fundamental rights (e.g., as regards direct access to their Personal Data and consent to its use or transfer).

Project Partners must apply the principle of data protection by design where it could mitigate the ethics risks raised by the data processing in Project Partners research Project and explain in the research proposal how this will be achieved. This approach is underscored by the principle of data protection by default. Wherever Project Partners have the possibility to enhance the level of data protection afforded to Project Participants, Project Partners should apply such measures by default rather than just considering them or making them available as an optional extra.

Where Project Partners research involves complex, sensitive or large-scale data processing, the proposal should include a description of the measures Project Partners will take to apply the principles of data protection by design and/or default to enhance security so as to prevent unauthorised access to Personal Data or equipment.

Informed Consent

Informed consent is the cornerstone of research ethics. It requires Project Partners to explain to research participants what the research is about, what their participation in the Project will entail and any risks that may be involved. Only after Project Partners have conveyed this information to the participants – and they have fully understood it – can Project Partners seek and obtain their express permission to include them in your Project (Articles 4(11) and 7 GDPR).

In principle, living individuals should not be the subject of a research Project without being informed, even in the rare cases where research methods, conditions or objectives dictate that they are not made fully aware of the nature of the study until its completion. However, the advent of the internet and the widespread use of social media platforms and other ICTs have dramatically expanded opportunities for researching human behaviour without the express consent of the subjects. In turn, this has created a range of ethical dilemmas and challenges for the research community.

Whenever Partners collect Personal Data directly from research participants, they must seek their informed consent by means of a procedure that meets the minimum standards of the GDPR. This requires consent to be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the subject's agreement to the processing of their Personal Data.6 This may take the form of a written statement, which may be collected by electronic means, or an oral statement.

Project Partners must keep records documenting the informed consent procedure, including the information sheets and consent forms provided to research participants, and the acquisition of their consent to data processing. These may be requested by data subjects, funding agencies or data protection supervisory authorities.

For consent to data processing to be 'informed,' the data subject must be provided with detailed information about the envisaged data processing in an intelligible and easily accessible form, using clear and plain language. As a minimum, this should include:

- the identity of the data controller and, where applicable, the contact details of the DPO;
- the specific purpose(s) of the processing for which the Personal Data will be used;
- the subject's rights as guaranteed by the GDPR and the EU Charter of Fundamental Rights, in particular the right to withdraw consent or access their data, the procedures to follow should they wish to do so, and the right to lodge a complaint with a supervisory authority;
- information as to whether data will be shared with or transferred to third parties and for what purposes; and
- how long the data will be retained before they are destroyed.

The data subjects must also be made aware if data are to be used for any other purposes, shared with research partners or transferred to organisations outside the EU (see article 13 GDPR).

As with any research Project involving human subjects, if the data processing entails potential risks to the data subjects' rights and freedoms, they must be made aware of these risks during the informed consent procedure.

The consent process(es) and the information Project Partners give to the data subjects should cover all the data-processing activities related to their participation in Project Partners research. From a research ethics perspective, and in accordance with the principles of fair and transparent data processing, if Project Partners intend to use or make their data available for future research Projects, it is best practice to obtain their additional, explicit consent to the secondary use of the data. If Project Partners do plan to use the data in multiple Projects or for purposes other than research, Project Partners must give the data subjects the opportunity to opt out of the further processing operation(s).

If in the course of research, Project Partners may wish to make any significant changes to the methodology or processing arrangements that have a bearing on the data subjects' rights or the use of their data. Hence, Project Partners must make them aware of the intended changes and seek and obtain their express consent; it is not enough to offer them the opportunity to opt out. This must be done before changes are made.

If the Project involves complex and large-scale data processing, if Project Partners plan to use the data in multiple Projects or for multiple purposes, or if it is not possible fully to identify the purpose of the data processing at the time of data collection, it may be appropriate to use a consent management application. Various service providers now offer ethically robust, secure informed consent platforms that can help Project Partners to manage, document and evidence Project Partners consent processes.

Data Protection Impact Assessments

The risk-based approach to data processing upon which the GDPR is predicated can help researchers with complex, sensitive or large-scale data processing requirements to identify and address the ethics issues that arise from their methods and objectives.

The DPIA is a process designed to assess the data-protection impacts of a Project, policy, programme, product or service and, in consultation with relevant stakeholders, to ensure that remedial actions are taken as necessary to correct, avoid or minimise the potential negative impacts on the data subjects.

Under the GDPR, a DPIA is mandatory for processing operations that are likely to 'result in a high risk to the rights and freedoms of natural persons'(art.35). These include in particular:

- ***Profiling, tracking, surveillance, automated decision-making and big data***

Widespread use and vast research and development potential of information and communication technologies has created a new range of ethical challenges. These include potentially adverse or unforeseen consequences for individual data subjects, specific communities and society at large. These may relate to the implications of combining and analysing different datasets, the potential for misuse of applications, or the risk of institutionalised discrimination.

If the research Project involves these techniques, Project Partners must provide a detailed analysis of the ethics issues raised by Project Partners methodology. This should comprise:

- an overview of all planned data collection and processing operations;
- identification and analysis of the ethics issues that these raises; and
- an explanation of how these issues will be addressed to mitigate them in practice.

If human participants participate in research studies, Project Partners must ensure that robust informed consent procedures are in place. Project Partners research involves human participants if Project Partners recruit them directly, or if Project Partners research activities consist of actively involving, influencing, manipulating or directing people in any way.

If the Project involves the large-scale processing of Personal Data using techniques such as data mining, 'web crawling' or social network analysis, Project Partners should address both the ethics implications of the research methods and the GDPR compatibility of the data processing.

If the Project involves the automated processing or profiling of Personal Data (see Box 6), Project Partners proposal should address the ethical implications of the objectives, methods and expected outcomes. Project Partners should also consider the legal, social and ethical impacts of any big-data analysis, eleven in particular its potential impact on people's right to equal treatment and non-discrimination.12

If the Project involves developing or using technology that may be used for the surveillance or tracking of individuals, it may fall within the scope of the EC dual-use regulation (428/2009) or be vulnerable to misuse. In such cases, Project Partners must consult the EC Guidance note-Research involving dual use items and/or EC Guidance note- Potential misuse of research.

If Project Partners Project entails the intensive monitoring or tracking of research participants, for example with regard to their movements, behaviour, activities or emotions, Project Partners proposal must explain what measures will be taken to protect both their Personal Data and fundamental rights.

If the goal of the Project is to develop surveillance technologies or techniques for law enforcement purposes, Project Partners proposal should explain why the surveillance can be deemed necessary and proportionate in a democratic society, in accordance with EU values, principles and laws.

As noted above, this kind of research may require a DPIA in accordance with the GDPR or supplementary guidance issued by supervisory authorities. If Project Partners planned research activities entail multiple or particularly complex ethics issues that cannot be resolved at the proposal stage, or subsequently through a DPIA, Project Partners proposal should make provision for a broader ethical impact assessment, which should in turn be subject to review by Project Partners research ethics committee or other appropriate body.

Data Security

Whenever and however Project Partners collect Personal Data, they have both ethical and legal obligations to ensure that participants' information is properly protected. This is fundamental to safeguarding their rights and freedoms and minimising the ethics risks related to data processing.

The GDPR requires all data controllers and processors to implement appropriate technical and organisational measures to ensure a level of data security that is commensurate to the risks faced by the data subjects in the event of unauthorised access to, or disclosure, accidental deletion or destruction of, their data (art.32 GDPR).

Project Partners proposal should provide details of the technical and organisational measures that will be implemented to protect the Personal Data processed in the course of Project Partners research, e.g., with reference to Project Partners host institution's and research partners' data protection and information security policies. Such measures may include the pseudonymisation and encryption of Personal Data, and policies and procedures to ensure the confidentiality, integrity, availability and resilience of processing systems.

Where higher-risk processing is envisaged (e.g., involving special categories or large-scale data), Project Partners should explain clearly how Project Partners will ensure an enhanced level of data security. In these scenarios, it is important that Project Partners choose appropriate research methods and data-processing tools (see Box 7).

This is vital where Project Partners research involves research subjects who are vulnerable or may be rendered vulnerable because of their participation in Project Partners research Project. This may be the case, e.g., if Project Partners are collecting data on sensitive political issues or communicating with people in countries with repressive governments. All communication is vulnerable to surveillance and interception,

but some channels are more susceptible than others. Wherever Project Partners believe there is a heightened risk to researchers and research participants, Project Partners should ensure that Project Partners communications are secure from unauthorised access.

Collection of Personal Data outside the European Union

Collecting Personal Data from research subjects in non-EU countries raises similar ethical issues, but these may be amplified by the need to ensure that the participants are:

- comfortable with being part of a research Project conducted by researchers from outside their own country;
- aware of what will happen to their data; and
- not subject to any undue pressure to participate.

As noted above, the EU's ethics requirements apply to all EU-funded research, irrespective of where it takes place. Similarly, the GDPR applies to all data-processing operations conducted by data controllers based in the EU, irrespective of where the processing takes place. This means that, even if Project Partners are collecting Personal Data outside the EU, Project Partners must still ensure and be able to demonstrate compliance with EU law.

Project Partners also have to comply with the laws of the country in which Project Partners are conducting Project Partners research, including any national data-protection laws. For example, Project Partners may be under an obligation to notify or seek permission for Project Partners research from national authorities or data protection regulators. Further authorisations may be required to transfer Personal Data outside the country in which the research takes place. 'Data sovereignty' provisions may even prohibit the transfer of certain kinds of information, such as health or patient data, out of the country.

Deletion and Archiving of Data

Project Partners may keep the Personal Data Project Partners collect only as long as it necessary for the purposes for which they were collected, or in accordance with the established auditing, archiving or retention provisions for Project Partners Project. These must be explained to Project Partners research participants in accordance with informed consent procedures.

Recent high-profile cases involving the misuse of Personal Data have stemmed from data controllers' failure to delete Personal Data and ensure that third parties to whom the data were provided had done the same in accordance with the agreed terms of their use.

As soon as Project Partners research data are no longer needed, or subject to an established retention period, Project Partners must securely delete the data in their entirety and make sure that they cannot be recovered. Data retained for auditing processes should be stored securely and further processed for those purposes only.

If research data are held in the cloud or by a third-party service provider, Project Partners should ensure that it has securely deleted the data together with any back-ups. If data have been shared with partners or transferred to third parties in the course of Project Partners Project, Project Partners should ensure that they have deleted the data, unless they have a legitimate basis for retaining them.

Data Protection Officers

If Project Partners institution has appointed a DPO, it is recommended that Project Partners seek their advice as to Project Partners data protection obligations and how to meet them. Project Partners must ensure that the DPO's contact details are made available to all the data subjects involved in Project Partners research.

If Project Partners Project raises complex data protection issues due to the sensitivity of the data, or the scale or nature of the processing involved, Project Partners should consider appointing a data protection specialist/adviser to Project Partners Project or research ethics board. If Project Partners host institution does not have a DPO, Project Partners should seek the advice of a suitably qualified expert in the preparation of Project Partners proposal and/or appoint such an expert to Project Partners Project if necessary.

If Project Partners need help and advice addressing the broader ethics issues raised by the data processing in Project Partners Project, Project Partners should contact the relevant institutional bodies or services (e.g., research office or research ethics committee) in Project Partners university or institution, relevant national bodies, members of Project Partners Consortium, or colleagues in Project Partners personal network who may have relevant expertise and experience.

If Project Partners are uncertain about any aspects of ethics in Project Partners research, Project Partners should consider appointing an ethics advisor or engaging an ethics mentor to provide advice, oversee the ethical concerns in Project Partners research and ensure that it is fully ethically compliant.

2.1 List of Project Partners

The partners forming part of this Project are the following and all are located within the European Union:

1) **ASSIST SOFTWARE SRL (AST)**, established in STR. TIPOGRAFIEI NR.1, SUCEAVA 720043, Romania;
2) **INSIKT INTELLIGENCE S.L. (INS)**, established in CALLE HUELVA 106, 9-4, BARCELONA 08020, Spain;
3) **IMAGGA TECHNOLOGIES LTD (IMG)**, established in ZH.K. MLADOST 4, BL. 471, VH. 4, AP. 120, SOFIA 1715, Bulgaria;
4) **ICON STUDIOS LTD (ICON)**, established in 1 MARINA COURT, OFFICE 4, TRIQ GIUSEPPE CALI, TA'XBIEX XBX 1421, Malta;
5) **CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI)**, established in VIA ARIOSTO 25, ROMA 00185, Italy;
6) **INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA)**, established in DOMAINE DE VOLUCEAU ROCQUENCOURT, LE CHESNAY CEDEX 78153, France;
7) **EOTVOS LORAND TUDOMANYEGYETEM (ELTE)**, established in EGYETEM TER 1-3, BUDAPEST 1053, Hungary;
8) **UNIVERSITA CATTOLICA DEL SACRO CUORE (UCSC)**, established in LARGO GEMELLI 1, MILANO 20123, Italy;
9) **MALTA INFORMATION TECHNOLOGY LAW ASSOCIATION (MITLA)**, established in SMARTCITY MALTA BUILDING SCM1001 RICASOLI, KALMARA SCM 1001, Malta;
10) **EUROPEAN INSTITUTE FOUNDATION (EI)**, established in G S RAKOVSKI STREET 101 SREDETZ DISTRICT, SOFIA 1000, Bulgaria;
11) **ASSOCIATION MILITANTS DES SAVOIRS (MDS)**, established in RUE EDMOND ROSTAND 24, TOULOUSE 31200, France,
12) **ETICAS RESEARCH AND CONSULTING SL (ETI)**, established in CALLE FERLANDINA 49, BARCELONA 08001, Spain;
13) **ELLINIKI ETAIRIA TILEPIKOINONION KAI TILEMATIKON EFARMOGON AE (NOVA – previously FNET)**, established in VASSILIKA VOUTON TECHNOLOGIKO PARKO, IRAKLEIO KRITI 71500, Greece;
14) **Ministério da Justiça (PJ)**, established in Praça do Comércio s/n, Lisboa 1149-019, Portugal;
15) **HOCHSCHULE FUR DEN OFFENTLICHEN DIENST IN BAYERN (HfoD)**, established in WAGMULLERSTRASSE 20, MUNCHEN 80539, Germany;
16) **IEKSLIETU MINISTRIJAS VALSTS POLICIJA STATE POLICE OF THE MINISTRY OF INTERIOR (SPLV)**, established in Ciekurkalna 1. linija 1, k-4, Riga LV-1026, Latvia;
17) **SERVICIUL DE PROTECTIE SI PAZA (SPP)**, established in B-dul GENIULUI, 42B, BUCURESTI 060117, Romania;
18) **GLAVNA DIREKTSIA NATSIONALNA POLITSIA (BGP)**, established in 1, ALEKSANDAR MALINOV BLVD., Sofia 1715, Bulgaria; and
19) **MINISTERE DE L'INTERIEUR (DGSI)**, established in Place Beauvau, PARIS, France 75800.

3 Legal Requirements

3.1 Executive Summary

The development, testing and pilot activities will naturally involve the collection of Personal Data throughout the Project's entirety. Hence, there is a legal obligation not only to conform to the most recent developments of European data protection laws, but also to ensure that the Project Partners can clearly and effectively demonstrate compliance with the above-mentioned laws.

It is important to note that this Deliverable addresses the requirements of the GDPR as they apply to the research and pilot stages of the Project. This Deliverable does not address the considerations which LEAs need to implement as per Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

3.2 Privacy and Personal Data Regulations

The GDPR is the most significant piece of legislation affecting the way that organizations carry out their information processing activities. The Project Consortium needs to ensure that its compliance with the GDPR is clear and demonstrable at all times of the Project.

Definitions

There are 26 definitions in total listed within the GDPR. The most important definitions within the context of the Project are as follows:

- 'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- 'processing' means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 'pseudonymisation' means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person;
- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union

or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; and

- 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

There are a number of principles upon which the GDPR is based, and these will guide the Project's activities:

(1) Personal Data shall be:
   a. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR, not be considered to be incompatible with the initial purposes ('purpose limitation');
   c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');
   d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
   e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); and
   f. Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

(2) The Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Some of the **key elements or changes** under the GDPR are:

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:
   a. The data subject has given consent to the processing of his or her Personal Data for one or more specific purposes;
   b. Processing is necessary for the 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. Processing is necessary for compliance with a legal obligation to which the controller is subject;

d. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
f. Processing is necessary for the purposes of the 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.

(2) **Extended Scope:** The GDPR applies to the processing of Personal Data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. The GDPR also applies to the processing of Personal Data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services or the monitoring of their behaviour as far as their behaviour takes place within the Union.

(3) **Increased administrative fines and penalties**: The penalties could reach out to €20 million or 4% of annual turnover at the organisation level.

(4) **Right to be forgotten** A data subject has the right to be forgotten, meaning that his/her Personal Data must be erased upon request, and no longer processed where the Personal Data is no longer necessary to the purposes for which it was collected, this subject to exceptions.

(5) **Right to access:** A data subject has the right to obtain from the data controller confirmation as to whether or not Personal Data concerning them is being processed, as well as details regarding the processing operation, such as the purposes of the processing, recipients, categories of Personal Data concerned, etc. The controller is required to provide a copy of the Personal Data, free of charge, in an electronic format.

(6) **Data portability:** A data subject has the right to receive the Personal Data concerning them; in a commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance.

(7) **Privacy by design and by default:** The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects; and

(8) **Breach notification:** Data Controllers are obliged to notify the supervisory authority of a Personal Data breach within 72 hours from becoming aware, and also the data subjects concerned where the Personal Data breach is of a high risk. Data Processors are obliged to notify the Data Controller without undue delay after becoming aware of a Personal Data breach.

3.3 Intended Purposes of Processing

As mentioned in section 4.2 above, Personal Data may only be used or otherwise processed in order to fulfil the purpose of its initial collection. Data controllers must ensure that Personal Data collected is not used for any purpose that is incompatible with its initial purpose. It is, therefore, vital for each Project partner, and the Consortium as a whole, to ensure that the purpose (or purposes) for which any Personal Data is collected are clearly established prior to the processing activity and such purpose must be subsequently communicated to the data subjects in question. The purpose of processing is typically set out within a privacy notice (a template of which is found in Appendix D and that privacy notice would need to be made available to the data subjects within a month from the collection of their Personal Data.

3.4 Legal Basis within article 6 of the GDPR

Once the purpose of processing has been determined for *each* processing activity due to be undertaken by the Project partners in accordance with section 4.3, the Project partners must ensure that the purpose of processing corresponds to at least one of the 'lawful bases' of processing set out under article 6 of the GDPR. If reliance cannot be placed on at least one of the lawful bases, then the Personal Data cannot be processed for the purpose in question.

The lawful bases of processing as set out within article 6 of the GDPR are reproduced below:

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her Personal Data for one or more specific purposes ('Consent);
b) processing is necessary for the 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 ('Contract');
c) processing is necessary for compliance with a legal obligation to which the controller is subject ('Legal Obligation');
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person ('vital interests');
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ('Public Interest'); and/or
f) processing is necessary for the purposes of the 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 ('Legitimate Interest').

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

In the context of the Project, the most applicable lawful basis when processing participant Personal Data will be Consent, as explained in greater detail in Section 5. In the event that the Project Partners identify Legitimate Interest as being the applicable lawful basis of consent, the Project Partners are encouraged to use the Legitimate Interest Assessment Template attached to this Deliverable as

Annex H, to ensure that the legitimate interest that they are pursuing does not override data subjects' fundamental rights and interests associated with the protection of their Personal Data.

3.5 Data Protection Officer

Article 31 GDPR requires a Data Protection Officer to be appointed as follows:

The controller and the processor shall designate a data protection officer in any case where:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and Personal Data relating to criminal convictions and offences referred to in Article 10.

In the circumstances, therefore, and given that the Project by its very nature aims at monitoring online and offline sources on a continual basis on a large scale, it is clear that the requirement to appoint a DPO to oversee the operations of the Consortium is mandatory. This obligation runs in parallel with that of the individual partners, and in particular those who process Personal Data, to appoint DPOs of their own to oversee their own internal operations.

The Consortium partners, with the exception of ETICAS and MITLA – who will not be processing any Personal Data –shall be guided by the Consortium's agreed upon Data Protection Officer ("**DPO**"). The DPO is Stefan Gavril, who will have overall responsibility for data management in CounteR and is the Data Protection Head of the Project.

3.6 Data Protection Guidelines to be followed by Project Partners

The Project partners that process Personal Data are subject to the requirements set out by the GDPR. The partners will meet all relevant EU legislation as well as national legal and ethical requirements of the countries where the tasks raising ethical issues are to be carried out. The ethical standards and guidelines of Horizon2020 will be complied with, regardless of the country in which the research is carried out. With respect to data collected and processed for the Project's scope, the following set of guidelines on potential compliance with ethical and privacy principles, will be followed:

- Where applicable, the data subject will be given a clear explanation about what data the Project collects, the purpose of the data collection, how the data collected will be used, stored and deleted.
- Personal Data shall not be processed unless the processing is based on a legal ground in accordance with the GDPR provisions.
- Where applicable, no Personal Data will be collected without data subject's consent, which consent shall be demonstrated by the Consortium partners through the use of approved consent forms created in Appendix E;

- No data will be collected that is expressly prohibited in terms of any law;
- All data that includes Personal Data will be transmitted (shared between partners) and stored in a secure manner;
- The data will only be stored for the duration that is necessary and for the purpose that it was designed;
- Only authorised persons from specific partners within the Consortium will have access to the Personal Data. This shall include Data Protection Officers in the exercise of their duties;
- Each partner will take all the measures necessary to ensure that effective data security and privacy provisions are fulfilled during the course of the Project lifecycle;
- The data will not be sold or used for any different purposes than the Counter Project;
- In pilot phase access to data will be restricted according to applicable regulations regarding data sharing;
- Data controllers will take appropriate confidentiality, integrity and availability measures to ensure protection (e.g., password protected limited access, regular back-up, encryption, etc.) for Personal Data processed within this Project;
- All the collected Personal Data will be stored on access restricted servers and secured against unauthorized access, accidental or unauthorized destruction, accidental loss as well as against unauthorized alteration or/and dissemination.
- At the end of the Project, all collected data for development and testing purposes will be deleted.
- Partners that work with Personal Data for its own developments and testing and in its own environment will follow the national legislation, H2020 provisions, GDPR and any applicable regulation and they will make the evidence of all the necessary arrangements, confirmation or/and copies of authorization.
- When the technical developments are not constrained by usage of Personal Data, fully anonymised data sets will be used and sharing of the data sets between partners will be based on anonymised data sets. The anonymisation is strongly recommended in order to avoid any data privacy issues regarding collection, storage, etc. related to Personal Data.
- Personal Data from questionnaires or workshops will be anonymised upon data collection by the organiser of the corresponding activity.
- If anonymisation of data sets is not technically feasible or possible because it negatively affects the performance of any devised solution, then specific rules will be applied between the partners, including any rules forming part of the Grant Agreement.
- Secure methods will be used for exchanging Personal Data between partners, including but not limited to, secure protocols, cryptography and more, in order to ensure the privacy and integrity.
- In the pilot phase, LEAs are most likely to use Personal Data to pilot and validate the system. In this case they will make the evidence of all the necessary arrangements, confirmation or/and copies of authorisation before the moment of starting these activities.
- If the collected data will be stored prior to anonymisation then the original data set will be destroyed after there is no need to keep the data set.
- The collected data sets will be limited to including only that information which is legitimately and exclusively required and necessary in order to complete the specified task.

- Data will be pseudonymised in order to maintain data access minimization for pilot phase.
- For Personal Data transfers between partners a Data Sharing Agreement Template was designed in order to be signed in the next period (Appendix F).

The above-mentioned provisions will be considered as strategies (procedures) to avoid misuse that will be implemented at the level of Project by all the partners.

Project Partners are encouraged to refer to Deliverable 1.3, which contains a review of the relevant supranational and EU laws and regulations applicable to each partner.

A basic template for Data Protection Policy provided by the IAPP (International Association of Privacy Professionals) and drafted by WhiteFuse is included as guidance in Appendix A. This template requires further elaboration from each partner that will need to consider the particular circumstances from its organisation and country and of the above-mentioned procedures. Therefore, each partner will need to consult their own legal counsel before finalising this policy.

4 Technical and Organisational Measures

4.1 Executive Summary

A technical or organisational measure and safeguard can be anything from the use of advanced technical solutions to the basic training of personnel[1]. Examples that may be suitable, depending on the context and risks associated with the processing in question, includes pseudonymization of Personal Data; storing Personal Data available in a structured, commonly machine readable format; enabling data subjects to intervene in the processing; providing information about the storage of Personal Data; having malware detection systems; training employees about basic "cyber hygiene"; establishing privacy and information security management systems, obligating processors contractually to implement specific data minimisation practices, etc[2]. This section sets out the importance of understanding the difference beetwen anonymization and pseudonymisation of Personal Data and the implications of each.

4.2 Anonymisation/Pseudonymization Techniques

4.2.1 Anonymisation vs Pseudonymization and the implications thereof

From a data protection perspective, it is imperative that all Project partners are aware of the difference between 'anonymisation' and 'pseudonymization' techniques under the GDPR.

According to the provisions of the GDPR and guidance issued in this respect, anonymization of Personal Data is an alternative to deletion, provided that all the relevant contextual elements are considered and the likelihood and severity of the risk, including the risk of reidentification, are regularly assessed[3]. Personal Data is only considered to be anonymised where the data has been stripped of sufficient elements such that the data subject can no longer be identified[4]. An additional consideration to bear in mind is that once this data has been anonymised, there must be no way of rendering the data subject (re) identifiable. If it is possible for the 'anonymised' data to be rendered identifiable at any point in time, that data is not deemed to be anonymised from a data protection perspective and therefore, the provisions of the GDPR continue to apply to it (even in its 'anonymised' state).

On the other hand, where Personal Data has been altered to as to render the data subject 'less identifiable', that Personal Data is said to have been subject to pseudonymization techniques. The GDPR defines 'pseudonymisation' as the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person[5]. This type of Personal Data is subject to the provisions of the GDPR and

[1] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*
[2] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*
[3] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*
[4] *Opinion 05/2014 on Anonymisation Techniques*
[5] *Article 4(5) GDPR*

is a way of ensuring that controllers have satisfied at least one of the principles of processing as set out in section 4.2(1)(f) above (integrity and confidentiality).

4.2.2 The importance of such techniques

The application of pseudonymisation to Personal Data can reduce the risks to the data subjects concerned and help data processing entities meet their data-protection obligations. While the principles of data protection continue to apply to pseudonymised data, they do not apply to anonymous information, namely information that does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In other words, the more Personal Data that is anonymised, the less exposure that the Project has from a GDPR perspective.

4.3 Minimum Requirements within ToMs

4.3.1 Definition of Technical and Organisational Measures

According to the EDPB's guidelines,[6] the term measures can be understood in a broad sense as any method or means that a controller may employ in the processing. These measures must be appropriate, meaning that they must be suited to achieve the intended purpose, i.e., they must be fit to implement the data protection principles effectively by reducing the risks of infringing the rights and freedoms of data subjects. The requirement for appropriateness is thus closely related to the requirement for effectiveness.

A technical or organisational measure can be anything from the use of advanced technical solutions to the basic training of personnel.[7] There is no requirement for the sophistication of a measure as long as it is appropriate for implementing the data protection principles effectively.

Safeguards act as a second tier to secure data subjects' rights and freedoms in the processing. Having implemented the data protection principles effectively means that the controller has integrated the safeguards that are necessary to ensure their effectiveness throughout the life cycle of the Personal Data being processed. Enabling data subjects to intervene in the processing, providing automatic and repeated information about what Personal Data is being stored, or having a retention reminder in a data repository may be examples of necessary safeguards. Another may be the implementation of a malware detection system on a computer network or storage system in addition to training employees about phishing and basic "cyber hygiene".

An example of a technical measure or safeguard is pseudonymization of Personal Data. Such a measure may be used to implement a number of principles, such as the integrity and confidentiality and data minimisation.[8]

[6] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*
[7] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*
[8] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*

4.3.2 Contractual Measures

The Consortium will need to assess how Project Partners are sharing Personal Data between themselves. If the relationship is deemed to be a joint controller one, the partners will need to enter into a joint controller agreement as mandated by article 26 of the GDPR. If, the Project Partners are deemed to be processing Personal Data in the context of controller – processor relationships, the partners will need to enter into a data processing agreement in accordance with article 28 of the GDPR.

If the partners are deemed to be neither joint controllers nor data processors, then it would be reasonable to conclude that the partners would be using Personal Data in their capacities as independent data controllers. The GDPR does not mandate for a written agreement to be implemented between independent controllers. However, it is advisable for the Project partners to implement the data sharing agreement set out in Appendix F between themselves so as to ensure that the way that they are each processing Personal Data conforms to a basic standard which conforms to the GDPR's requirements.

4.3.3 Compliance Checklist

As a starting point, Project partners are encouraged to utilise the checklist set out below in order for them to assess their level of compliance with the principle of integrity and confidentiality, as well as article 32 of the GDPR. This checklist was published by the Information Commissioner's Office (the data protection authority in England), and it serves as a useful starting point for controllers as it highlights any gaps which controllers may have in respect of the security over their Personal Data[9]:

- We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- Where necessary, we have additional policies and ensure that controls are in place to enforce them.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We have assessed what we need to do by considering the security outcomes we want to achieve.
- We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of Personal Data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the Personal Data we process.

[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

- We make sure that we can restore access to Personal Data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

5 Issues regarding Consent

5.1 Executive Summary

Obtaining participant's informed consent is a requirement when conducting research utilising Personal Data, particularly when monitoring, crawling and mining of data is involved. Hence, it is imperative to provide participants with a detailed description of the way in which research will be conducted and how their Personal Data will be processed throughout the Project's entirety.

5.2 Introduction to Consent

5.2.1 EDPB Guidelines

The European Data Protection Board ("EDPB") published Guidelines 05/2020 on consent under Regulation 2016/679 (the "**Guidelines**") which were adopted on 4 May 2020. The Guidelines are available here: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

It is advisable for all Project partners to familiarise themselves with the Guidelines and ensure that each Project partner complies with the local data protection law which it is subject to.

The introduction to the GDPR explains that consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of Personal Data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her Personal Data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

5.2.2 Freely Given

One of the most important aspects of the collection of valid consent from a GDPR perspective is that such consent is freely given by the data subject. This means that the data subject should not feel or think that he or she has no real choice but to consent or feels compelled to consent[10]. Furthermore, the data subject should not feel as if they will suffer negative consequences if they do not consent to their processing of Personal Data[11].

[10] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[11] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

When assessing whether consent is freely given, the partners should take into account the specific situation of tying consent into contracts, or the provision of a service as described in Article 7(4). In general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.[12]One such example is if the data subject feels like there is an imbalance of power between themselves and the data controller.

In summary, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g., substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will[13].

5.2.3 Specific

The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject. This requirement is closely linked to the requirement of 'informed' consent. At the same time, it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent. In sum, to comply with the element of 'specific' the controller must apply:

a) Purpose specification as a safeguard against function creep;
b) Granularity in consent requests; and
c) Clear separation of information related to obtaining consent for data processing activities from information about other matters.

If the controller is relying on Consent, data subjects must always give consent for a specific processing purpose. In line with the concept of purpose limitation as explained in section 4.3, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis, which better reflects the situation.

5.2.4 Informed

The GDPR reinforces the requirement that consent must be informed. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory, and consent will be an invalid basis for processing. The consequence of not complying with

[12] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[13] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

the requirements for informed consent is that consent will be invalid, and the controller may be in breach of Article 6 of the GDPR.

Informed consent is fundamental in conducting field trust in an ethical and lawful manner. Project participants must be provided with the Informed Consent Template (as provided in D11.1) and Data Privacy Notice in Appendix E and Appendix D, respectively. As previously mentioned, it is imperative that any information provided to Project Participants:

a) are written in a language and in terms they can fully understand;
b) describe the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomfort that might ensue;
c) explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time —without any consequences;
d) state data will be collected, protected during the Project and either destroyed or reused subsequently;
e) state what procedures will be implemented in the event of unexpected or incidental findings (in particular, whether the participants have the right to know, or not to know, about any such findings).

5.2.5 Obtaining Explicit Consent

The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. Explicit consent is particularly necessary where serious data protection risks emerge when assessing the processing activities that are taking place.

The particular situations in which explicit consent is required are where:

a) the processing of special categories of data is taking place;
b) data is being transferred to third countries or international organisations in certain situations; and
c) data is being processed using automated individual decision-making, including profiling.

Seeing as the Project is likely to consist of processing using automated decision making (including profiling), explicit consent will be required to be collected before any Personal Data can be fed into the Counter solution.

An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Other methods through which explicit consent may be obtained are:

a) Two stage verification of consent;
b) through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g., pressing a button or providing oral confirmation); and
c) in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature.

5.2.6 Additional Conditions

The GDPR introduces requirements for controllers to make additional arrangements to ensure they obtain, and maintain and are able to demonstrate, valid consent. Article 7 of the GDPR sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent.

Controllers are free to develop methods relating to record keeping in a way that fits in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they should not be collecting any more information than necessary. It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented and this obligation subsists for as long as the processing activity in question lasts. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action. However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels. As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g., further storage) of the data, they should be deleted by the controller.

5.2.7 Interplay between Consent and other Legal Bases

As explained above, Consent is only one of six lawful bases set out under article 6 of the GDPR. Typically, consent is left as a lawful bases of last resort when determining the appropriate lawful bases of processing for a particular processing activity. This is mainly because of the requirements that controllers must comply with in order for Consent to be validly collected. However, there are instances in which Consent is the only valid lawful basis of processing, notwithstanding the number of stringent requirements needing to be satisfied. In the context of the Project, particularly in respect of participant Personal Data, Consent will be the only applicable lawful basis of processing which Project partners can rely on when collecting such participants' Personal Data.

5.3 Nuances within the Data Supply Chain

5.3.1 Clearnet

For a detailed review of the technical requirements relating to the Project, kindly refer to Deliverable 1.2. It is important to note that even if Personal Data is collected from publicly available or open-source locations, the provisions of the GDPR shall continue to apply to that information, to the extent that the information contains Personal Data. Moreover, unless a lawful basis under article 6 of the GDPR can be identified (as explained in section 4.4 above), it is not lawful to collect or otherwise use Personal Data collected from such sources.

5.3.2 Dark Web

For a detailed review of the Dark Web collection tool intended to be developed by the Project, kindly refer to Deliverable 1.2. From a data protection perspective, even though information would be collected from a publicly available source, it is important to note that the provisions of the GDPR continue to apply to the Personal Data and therefore, the Consortium would need to identify a lawful basis of processing (as explained in section 4.4 above), before this data is collected. Furthermore, the Consortium needs to consider the use of Personal Data collected from the dark web in the context of the principles of processing (as described in section 4.2(1) above). The principle that causes the most concern at this juncture is the principle of 'lawfulness, fairness and transparency'. This is because in general terms, data placed on the dark web has been placed there illegally and therefore, the Consortium must consider how this Personal Data is going to be extracted and used for the legitimate purposes of the Project, while at the same time satisfying the requirements of the GDPR.

In light of this section 6.3.2 and 6.3.1 above, it is important for the Consortium to conduct a DPIA (as explained in section 7 below) in order to assess how the Project is going to manoeuvre this prohibition, while respecting and protecting the Personal Data of all data subjects concerned.

6 Ethical Guidelines

6.1 Ethical Approach

This section describes the ethical and responsible research principles that should guide the Project. Project Partners must carry out their research in compliance with ethical principles, including the highest standards of research integrity. Moreover, they must follow EU, national law during the Project's test-phase, and conform to the H2020 ethics standards and guidelines.

In line with the European Code of Conduct for Research Integrity (All European Academies, 2017),[14] this means compliance with the principles of honesty, reliability, objectivity, impartiality, open communication, duty of care, fairness and responsibility for future science generations. Hence, Project Partners must ensure that persons carrying out research tasks:

- Present their research goals and intentions honestly and transparently;
- Design their research carefully and conduct it reliably, taking its impact on society into account;
- Use techniques and methodologies (including for data collection and management) that are appropriate for the field(s) concerned;
- Exercise due care for the subjects of research — be they human beings, animals, the environment or cultural objects;
- Ensure objectivity, accuracy, and impartiality when disseminating the results;
- Allow — as much as possible and taking into account the legitimate interest of the beneficiaries — access to research data, in order to enable research to be reproduced;
- Consider the potentially sensitive nature of the research and refrain from publishing or disseminating research results, datasets or protocols that might be misused, infringe on the rights of others or cause harm to the persons involved;
- Make the necessary references to their work and that of other researchers;
- Refrain from practising any form of plagiarism, data falsification or fabrication; and
- Avoid double funding, conflicts of interest and misrepresentation of credentials or other research misconduct.

Ethical Governance in CounteR

The Project Coordinator (ASSIST) and WP7 members (ETICAS and MITLA), acting as Ethics Advisors (EEA), will assure good ethical governance of the Project. These partners are responsible for ethics monitoring, and are the contact person for members of the Project on everything regarding research ethics (ethics protocols, information sheets, consent forms, reporting, supervising the demos, etc.). Moreover, they are responsible for presenting all relevant documents to the Security Advisory Board (SAB) for them to review.

[14] *ALLEA (2017). The European Code of Conduct for Research Integrity. Berlín: All European Academies.*

The EEA members will have to provide advice and suggestions on the Project's solutions and results of the Project to the rest of the CounteR Consortium. Furthermore, EEA members will provide feedback and advice on Project research development's data protection and ethical issues. Finally, EEA members will also offer open consultation on specific ethical questions if needed and upon request.

Ethical Framework for CounteR Research Activities with Human Participants

The Ethical framework consist of a set of procedures to be followed in addressing ethical issues, criteria to be factored into a decision, or both. An essential goal of the Project is to develop and validate a situational awareness platform to counter violent terrorism. As addressed in Deliverable 7.1, testing these systems with real data during the research development and implementing them is challenging from the ethical and data protection standpoints. Therefore, the European Security Model's concerns (e.g., perception of security, possible side effects of technological solutions, cross cutting issues involving Social Sciences and Humanities (SSH) and gender- and age-related behaviour) will be of utmost importance for the Project's development.

Regarding human participants in CounteR, their rights to autonomy, integrity and privacy -rights recognized by international law and all EU Member States- must be respected. The Declaration of Helsinki (World medical Assembly, 1964), and The Belmont Report (The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1978) represent standards for research aligned with these legal frameworks. The Nuremberg Code underlined the need to assure the voluntary nature of human participation in research and pointed out the requirement of establishing instruments for informed consent, guaranteeing that people involved in research can withdraw from it whenever they want. Wellbeing and interests of participants must be protected, and researchers must establish mitigation measures for addressing any risk of harm for them.

The Belmont Report established four key ethical principles to be considered when carrying out research activities:

- **respect for people**: research subjects must be treated protecting their safety, respecting their autonomy and ensuring their consent on an informed basis,
- **beneficence**: possible benefits for the participants will be maximized while possible harm or risk will be minimized,
- **justice**: any benefits and burdens derived from research must be weighted,
- **competence**: the limitations and boundaries of the researcher competence must be recognized and made explicit.

In CounteR, operationalizing these principles has specific implications since certain tests can potentially affect the health and wellbeing of participants, primarily by violating their right to privacy. Regarding Project Participants, care must be taken to verify that such have not been coerced into participating, including their employers, family, or relatives. In this regard, their rights must be clear from the informed consent form. Researchers may also clearly explain these procedures to Project Participants, ensuring that they have understood. The information imparted to the Project Participants must be clear and provide sufficient information so as not to deceive them. They need to understand what they agree to. Researchers must make sure that Project Participant's Personal Data is properly protected from unauthorized access. The more sensitive the

data, the more measures need to be in place. When disseminating research results, care must be taken to make sure no participant can be individually identified.

The Project's methodology involves consultation (through interviews, questionnaires and workshops) with Practitioners-Stakeholders (e.g. LEAs) and an analysis of the system data protection and acceptability in WP7. One of the main objectives of the Project is contributing to people's safety. However, monitoring big data online requires ensuring respect for privacy, setting mechanisms for ensuring non-discrimination and prevention of misuse. In this respect, in creating the ethical and legal governance framework for CounteR research activities, we have considered the ethical principles related to crime prevention online. The Consortium will seek to implement five ethical goals designed to inform both the content of prevention plans and the process by which they are devised, updated, and implemented (Jennings and Arras, 2008)[15]:

1) **Harm reduction and benefit promotion**. Crime prediction and online response activities should protect public safety, health, and well-being. They should minimize the extent of death, injury, disease, disability, and suffering during and after an emergency.
2) **Equal liberty and human rights**. Crime prediction and online response activities should be designed so as to respect the equal liberty, autonomy and dignity of all persons.
3) **Distributive justice**. Crime prediction and online response activities should be conducted so as to ensure that the benefits and burdens imposed on the population by the need to cope with its effects are shared equitably and fairly.
4) **Public accountability and transparency**. Crime prediction and online response activities should be based on and incorporate decision-making processes that are inclusive, transparent, and sustain public trust.
5) **Responsible civic response**. Crime prediction and online response activities should promote a sense of personal responsibility and citizenship.

These ethical issues need to be addressed transversally to all Project activities. For example, integral to the question of capturing and analysing individuals and group behaviours online is the achievement of a balance between a citizen's right to privacy and their right to be safe and secure. Aware of the potential ethical issues mentioned above, Project CpunteR has built ethical, legal and social safeguards for the proposed technical solutions and methodologies, which will be screened based on the following ethical compliance checklist.

[15] *Jennings B, Arras J, (2008) Ethical Guidance for Public Health Emergency Preparedness and Response: Highlighting Ethics and Values in a Vital Public Health Service, available at https://www.semanticscholar.org/paper/Ethical-guidance-for-public-health-emergency-and-%3A-Jennings-Arras/01430218c871b8df2d0d41be63617dab415301ed*

6.2 Ethical Compliance Checklist

The aim of this Checklist is to ascertain the Project's compliance with the Horizon 2020 Ethical Standards Manual.The Project Partners are encouraged to analyse the below and utilise the Checklist as a tool to assist their thought-process in developing the CounteR solution.

Kindly note, at this stage, the Project is still under development. the Ethics Briefing Pack 2nd Version (M22) will provide detailed guidance on the solution's requirements, in line with the Project's technical requirements and legal feasibility thereof.

Review question	Status			Comments
CounteR Governance				
Does the CounteR Project have an approved DMP and ethical guidelines?	Yes ☒	No ☐	NA ☐	• Deliverables D10.3, which has been finalised and uploaded to the shared cloud environment. • Ethical guidelines may be found within WP 7 and 11, respectively. The respective Deliverables are still in development and will be finalised and uploaded to the cloud by 31 December.
Has the data management plan and the ethical guidelines been reviewed by all stakeholders?	Yes ☒	No ☐	NA ☐	• All Deliverables go through an internal review before submission to ensure partners contributions and approval.
Are roles and responsibilities of Project stakeholders allocated and defined among such?	Yes ☒	No ☐	NA ☐	• CounteR data sharing agreement. • Deliverables handled by Respective Project Partners. • During plenary and virtual meetings, responsibilities have been allocated to partners.
Do CounteR representatives have the necessary knowledge, expertise and the competence to conduct the pilots?	Yes ☒	No ☐	NA ☐	• CounteR representatives will/have been trained staff, particularly LEAs, and are ready to respond to any issue that may appear in the process. • Training sessions of best data processing and privacy/ethical practices are to be conducted closer to trials.
Should CounteR representatives have a conflict of interest, is there an adequate plan to eliminate it or manage it appropriately?	Yes ☒	No ☐	NA ☐	• Self-assessment audit form. • Written confirmation that the Consortium has no conflict of interest with the appointed ethical experts. • Appropriate regulation of NDAs within employment contracts.
Does the Project adequately explain how Personal Data **("PD")** is to be acquired, handled, stored and disseminated?	Yes ☒	No ☐	NA ☐	• Sections 2/3/5/6 of the DMP does not envisage the processing of SCPDs.

Where special categories of PD **("SCPDs")** are collected, does the Project indicate why they are needed and what security measures are in place to ensure they are adequately protected?	Yes ☐	No ☐	NA ☒	• The DMP does not envisage the processing of SCPDs. D7.1 provides relevant definitions and legal requirements regarding safeguards to be taken when managing special categories of data.
Are there adequate provisions to maintain the confidentiality of the identifiable data?	Yes ☒	No ☐	NA ☐	• Section 5 of the DMP lists the security measures to be utilised throughout the Project. • Appendix B/C of the DMP list certain Deliverables as confidential or classified, respectively.
Has a Data Protection Impact Assessment been performed by CounteR to assess the risk to privacy and data protection?	Yes ☒	No ☐	NA ☐	• The DPIA is currently being developed within WP7 and will be finalised by the respective Due Date.
CounteR privacy notice				
Is the CounteR privacy notice written in understandable non-technical languages?	Yes ☒	No ☐	NA ☐	• This is also explained throughout the various meetings and information on how to utilise the respective Deliverables has been provided to Project Partners.
Does the Project information sheet state clearly if it is a research study?	Yes ☒	No ☐	NA ☐	• This particular point is handled throughout various Deliverables within different WPs.
Does the Project information sheet explain the purpose of the research and pilots?	Yes ☒	No ☐	NA ☐	• The respective purpose is handled within the DMP itself, alongside WP7 and WP11. Please note that this requires updating as the Project evolves. MITLA is contributing to these discussions in order to finalise these.
Does the Project information sheet clearly describe procedures to be followed and preformed and which of these are experimental?	Yes ☒	No ☐	NA ☐	• Sections 2/3 and Appendices A/D of the DMP describe such procedures.
Does the CounteR privacy notice describe why the participant (subject) is qualified or not for the pilots?	Yes ☒	No ☐	NA ☐	• Deliverable D11.1 H will identify and detail such procedures, including the qualification requirements of participants.
Does the CounteR privacy notice clearly state the time and/or commitments required of participants?	Yes ☒	No ☐	NA ☐	• WP 7 will specify any commitments and supplementary requirements from participants.
Does the CounteR privacy notice provide points of contact for further information if participants require to contact CounteR regarding their rights?	Yes ☒	No ☐	NA ☐	• Each LEA is instructed to include their DPO details within the Privacy Notice Template. • Please note that there cannot be one single, over-arching Privacy Notice. Rather, each LEA or Project Participant is to update the PN within Deliverable WP 7 and include their respective DPO.

Does the CounteR privacy notice provide a description of any benefits or risk to the participants?	Yes ☒	No ☐	NA ☐	• Including risk-analysis within the PN is not within the scope of Art. 13 GDPR. • Rather, LEAs will have prior knowledge of such benefits and risks, through WP7 and WP11, which should be cascades to the respective Participant Project.
Does the CounteR privacy notice provide a statement that the participating is voluntary and the subject many refuses to participate without penalty or loss of benefits to which the subject is otherwise entitled?	Yes ☒	No ☐	NA ☐	• This has been implemented accordingly.
Does the CounteR privacy notice clearly describe how the Personal Data will be protected to ensure subject's privacy and confidently?	Yes ☒	No ☐	NA ☐	• Yes. Additionally, this is listed within Sections 5 and 6 of the DMP. • The specific technical & organisational measures are yet to be agreed upon by the Project Partners. • However, each Partner would have already included their own respective ToMs throughout the Project's lifespan.
Does the CounteR information sheet clearly describe how the result will be disseminated and published?	Yes ☒	No ☐	NA ☐	• Yes. Additionally, this will be listed within Deliverable D9.3 once the Deliverable has been finalised.
CounteR informed consent				
Does the consent form clearly describe the Project's purpose, procedures to be followed, benefits etc.?	Yes ☒	No ☐	NA ☐	• Yes. This is both described within WP7, WP11 and Section 6 of the DMP.
Will the informed consent be obtained prior to pilots?	Yes ☒	No ☐	NA ☐	• The informed consent template will be provided to the necessary participants, prior to the pilots being initiated.
Will the participants given a sufficient opportunity and time to consider whether or not to consent?	Yes ☒	No ☐	NA ☐	• As detailed before, consent is handled on an individual basis by the LEAs, who provide the Project Participants with engagement/employment contracts prior to their engagement within the Project.
Is the consent form specific for the purpose of CounteR pilot?	Yes ☒	No ☐	NA ☐	• This has been specified within the Data Sharing Agreement, Informed Consent Template, and DMP.
Does CounteR consent form provide a statement that participating is voluntary and the subject may withdraw without penalty or loss of benefits to which the subject is otherwise entitled?	Yes ☒	No ☐	NA ☐	• This information is included both within the Informed Consent Template, as well as the Data Sharing Agreement and Privacy Notice.

Will participants be given enough information about the withdrawal procedures and how to withdraw from pilots if they wish?	Yes ☒	No ☐	NA ☐	• This information is included both within the Informed Consent Template, as well as the Data Sharing Agreement and Privacy Notice.
Is the signature of the participant required and recorded?	Yes ☒	No ☐	NA ☐	• Yes, both within the employment contracts, and also within the Informed Consent Template.
Is the signature of the CounteR representatives who collected the consent required and recorded?	Yes ☒	No ☐	NA ☐	• The final deliverable has not yet been published but will reflect this requirement and include a field for the signature of the respective representative.

7 Data Protection Impact Assessment

7.1 Legal Requirements of a DPIA

Where a type of processing in particular using new technologies, and considering the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data. The GDPR states that a DPIA shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1) GDPR, or of Personal Data relating to criminal convictions and offences referred to in Article 10 GDPR; or
c) a systematic monitoring of a publicly accessible area on a large scale.

Furthermore, the WP29's guidelines entitled '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' (endorsed by the European Data Protection Board) stipulate that a DPIA would be required to be undertaken where processing involves the matching or combining of datasets.

The Project clearly satisfies the requirements set out above and therefore, a DPIA should be conducted by the Consortium prior to the utilisation of the solution by the LEAs within the pilot phase.

It is important to note that data protection authorities in each member state of the European Union is likely to have its own requirements as to when a DPIA is expected to be carried out. Each Partner is, therefore, encouraged to consult with their own data protection authority in order to ensure that DPIAs are being undertaken where necessary.

7.2 How to Conduct a DPIA

DPIAs must contain at the least the following:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with this Regulation considering the rights and legitimate interests of data subjects and other persons concerned.

In order to conduct a DPIA, the first step is to identify the different types of Personal Data being processed, and how that data is being collected. Once this has been established, it is then important to determine what the purposes of processing are, and the lawful basis being relied upon. While undertaking the DPIA, it is important to keep the four points mentioned in a-d of this section in mind so as to assess the necessity and proportionality of the processing, as well as the risks.

Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller must consult with the relevant data protection authority in accordance with article 36 of the GDPR.

7.3 Policies and Procedures

One of the most important principles of processing is the principle of 'accountability', whereby data controllers are able to demonstrate the steps that they have taken in order to comply with the GDPR. One of the most effective ways of demonstrating accountability is to implement and maintain internal policies and procedures. These policies and procedures include:

a) Clean desk policy;
b) IT security policy;
c) Website use policy; and
d) Cookie's policy.

The Deliverable also includes an Access Policy Appendix B which explains how the partners are expected to respond to data subject access requests, and a Retention Policy Appendix C, which sets out the considerations which the Project would need to consider when setting the retention periods of the Personal Data being processed.

It is advisable for every Project partner to implement relevant policies and procedures to ensure that the are adhering to the principle of accountability under the GDPR, as well as the principles of data protection by design and by default as set out within article 25 of the GDPR.

8 Conclusions

Data protection compliance is an ongoing task and is expected to remain a key priority throughout the entire lifespan of the Project. This deliverable is directly related to Task 7.4 in WP7, due at the end of the Project, which will examine the practices and procedures that have been adopted by the Consortium in the development of its work and will assess how these are compliant with applicable privacy laws. It is for this reason that the work of partner DPOs will be indispensable in ensuring that the Consortium remains focused not only on working on its principal aim of finding a solution which the Project seeks to achieve, but also by keeping legal and ethical principles at the core of its work at all times.

Appendix A: Data Protection Policy

[Insert entity name]

Note about this policy template: Lots of template policies are unhelpfully long and simply reiterate large portions of the legislation. This template is different: it aims to provide a concise and practical document that can be used by trustees of small entities as the foundation for a working Data Protection Policy. If you have any doubt about your legal obligations, you should always check with the MITLA teams, or your national legislation if so required.

Last updated:

Definitions:

"**Data Protection Legislation**"	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data by competent authorities for the Intended Purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA and all relevant National Legislation.
"**End of Project**"	mean the date upon which the CounteR Project has been officially finalised. As per the Grant Agreement, the Project's end date shall be 1st May 2023.
"**National Legislation**"	means all national legislation which is applicable to the [Project Partner] by virtue of the relevant jurisdiction.
"**Personal Data**"	means any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number, location data or online identifier.
"**Processing**"	means any operation or set of operations that is performed on Personal Data, such as collection, use, storage, dissemination, and destruction.
"**Retention Period**"	means the duration (in months or days, as applicable), which is applicable to the respective: Category/Specific of Personal Data.
"**Project Partner**"	means [Project Partner], a registered Entity as per the GA.
"**Responsible Person**"	means [insert entity DPO].
"**Register of Systems**"	means a register of all systems or contexts in which Personal Data is Processed by [Project Partner].

1. Data protection principles

The Entity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that Personal Data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. General provisions

a) This policy applies to all Personal Data processed by [Project Partner].
b) The Responsible Person shall take responsibility for [Project Partner]'s ongoing compliance with this policy.
c) This policy shall be reviewed at least annually.
d) [Project Partner] shall register with the [insert name of national Data Protection Authority]as an organisation that processes Personal Data.

3. Lawful, fair and transparent processing

a) To ensure its processing of data is lawful, fair and transparent, the Entity shall maintain a Register of Systems.
b) The Register of Systems shall be reviewed at least annually.
c) Individuals have the right to access their Personal Data and any such requests made to [Project Partner] shall be dealt with in a timely manner.

4. Lawful purposes

a) All data processed by [Project Partner] must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (refer to your national Data Protection Authority for more guidance on this).
b) [Project Partner] shall note the appropriate lawful basis in the Register of Systems.
c) Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the Personal Data.
d) Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in [Project Partner]'s systems.

5. Data minimization

a) [Project Partner] shall ensure that Personal Data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b) [Add considerations relevant to Project Partner's particular systems]

6. Accuracy

a) [Project Partner] shall take reasonable steps to ensure Personal Data is accurate.
b) Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that Personal Data is kept up to date.
c) [Add considerations relevant to the [Project Partner]'s particular systems]

7. Archiving / removal

a) To ensure that Personal Data is kept for no longer than necessary, [Project Partner] shall put in place an archiving policy for each area in which Personal Data is processed and review this process annually.
b) The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a) [Project Partner] shall ensure that Personal Data is stored securely using modern software that is kept-up to date.
b) Access to Personal Data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c) When Personal Data is deleted, this should be done safely such that the data is irrecoverable.
d) Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, [Project Partner] shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the (insert name of national Data Protection Authority, and URL to that Authority's website).

Appendix B: Access Policy

Data Subject Access Request Procedure

LAST UPDATED: [-]

1. About this procedure

1.1. We, [insert name of Project partner] (hereinafter referred to as "We", "Our" and "Us"), have adopted this Data Subject Access procedure which provides a framework for responding to requests from data subjects to exercise their right of access to Personal Data concerning him or her. It is Our responsibility to ensure that such requests are handled in terms of applicable law.

1.2. For the purpose of this procedure:

"**applicable law**"	means the EU General Data Protection Regulation (2016/679) ("GDPR") and any other national data protection law applicable to Us.
"**Personal Data**"	means any information relating to an identified or identifiable natural person ("data subject"). A data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number, location data or online identifier; and
"**process, processing**"	means any operation or set of operations that is performed on Personal Data, such as collection, use, storage, dissemination and destruction.

1.3. This procedure only applies to data subjects whose Personal Data We process.

2. Responding to requests to access Personal Data

2.1. Data subjects have the right to request access to their Personal Data processed by Us by making subject access requests ("**SARs**") addressed to Us. When a data subject submits a SAR, the following steps shall be taken:

a. We shall immediately inform the Consortium of the request;
b. log the date on which the request was received (to ensure that the relevant timeframe of one (1) month for responding to the request is met);
c. confirm and verify the identity of the data subject who is the subject of the Personal Data. For example, when necessary for verification and confirmation of identity We may request additional information from the data subject such as by requesting such data subject to fill in Our Data Subject Access Request Form, annexed hereto as Annex A;
d. search databases, systems, applications and other places where the Personal Data which are the subject of the request may be held; and
e. confirm whether or not Personal Data of the data subject making the SAR are being processed by Us.

2.2. If Personal Data of the data subject are being processed, We shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

a. the purposes of the processing;
b. the categories of Personal Data concerned (for example, contact details and details of sales activity);
c. the recipients or categories of recipient to whom the Personal Data have been or will be disclosed;
d. where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
e. the existence of the right to request rectification or erasure of Personal Data or restriction of processing of Personal Data or to object to such processing;
f. the right to lodge a complaint with Our supervisory authority;
g. where the Personal Data are not collected from the data subject, any available information as to their source; and
h. the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2.3. We shall also, unless there is an exemption (see section 3 below), provide the data subject with a copy of the Personal Data processed by Us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one (1) month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two (2) months. If we extend the period for responding we shall inform the data subject within one (1) month of receipt of the request and explain the reason(s) for the delay.

2.4. Before providing the Personal Data to the data subject making the SAR, We shall review the Personal Data requested to see if the said Personal Data contain Personal Data of other data subjects. If so, We may redact the Personal Data of those other data subjects prior to providing the data subject with their Personal Data, unless those other data subjects have consented to the disclosure of their Personal Data.

2.5. If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, We may charge a reasonable fee, considering the administrative costs of providing the Personal Data, or refuse to act on the request.

2.6. If We have determined that we are justified in not responding to the SAR We shall inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the relevant supervisory authority.

3. Exemptions

3.1. Before responding to any request, We shall check whether there are any exemptions that apply to the Personal Data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above to safeguard:

a. national security;
b. defence;
c. public security;
d. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e. other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;
f. the protection of judicial independence and judicial proceedings;
g. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in paragraph 3.1a and paragraph 3.1g above;
i. the protection of the data subject or the rights and freedoms of others; or
j. the enforcement of civil law claims.

Annex A

Data Subject Access Request Form

Article 15 of the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") grants you the right to access your Personal Data held by [insert name of Project partner], including the right to obtain confirmation that We process your Personal Data, receive certain information about the processing of your Personal Data, and obtain a copy of the Personal Data We process.

We require that you submit this request in writing via postal mail at [-] or electronically via email to [insert relevant details].

We expect to respond to your request within no later than one (1) month of receipt of a fully completed form and proof of identity. This notwithstanding, we reserve the right to extend the period for responding by a further two (2) months if your request is complex or you have submitted more than one request.

In addition to exercising your access right, the GDPR also grants you the right to:

a) request correction or erasure of your Personal Data;
b) restrict or object to certain types of data processing; and
c) make a complaint with our supervisory authority.

For more information on your rights under the GDPR, see our Privacy Notice available at: [*Insert location of where the Privacy Notice can be found*].

I. Data Subject Name and Contact Information

Please provide your information in the space provided below. If you are making this request on the data subject's behalf, you should provide your name and contact information in Section III.

We will only use the information you provide on this form to identify you and the Personal Data you are requesting access to, and to respond to your request. Once this request has been concluded, this form shall be irrevocably deleted.

Name and Surname:	
Any other names that you have been known by (including nicknames):	
ID/Passport number:	
Address:	
Date of birth:	
Telephone/Mobile number:	
Email address:	
Please provide any related information which can help us locate your Personal Data:	

II. Proof of Data Subject's Identity

We require proof of your identity before We can respond to your access request. To help Us establish your identity, you must provide identification that clearly shows your name, date of birth, and current address. We accept a photocopy or a scanned image of one (1) of the following as proof of identity: passport, driver's license or ID card. If you have changed your name, please provide the relevant documents evidencing the change. Once your identity has been verified, the Personal Data that you have provided Us with for the purpose of your verification shall be immediately and irrevocably destroyed.

If you do not have any of these forms of identification available, please contact [-] for advice on other acceptable forms of identification.

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the Personal Data We hold about you. We reserve the right to refuse to act on your request if We are unable to identify you.

III. Requests Made on a Data Subject's Behalf

Please also complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

Name and Surname:	
ID/Passport Number:	
Address:	
Date of birth:	
Telephone/Mobile number:	
Email address:	

We accept a photocopy or a scanned image of one (1) of the following as proof of your identity: passport, driver's license or ID Card. If you do not have any of these forms of identification available, please contact [-] for advice on other acceptable forms of identification. We may request additional information from you to help confirm your identity if necessary.

We also require proof of the data subject's identity before We can respond to the request. To help Us establish the data subject's identity, you must provide identification that clearly shows the data subject's name, date of birth, and current address. We accept a photocopy or a scanned image of one (1) of the following as proof of identity: passport, driver's license or ID Card. If the data subject has changed name, please provide the relevant documents evidencing the change.

We accept a copy of the following as proof of your legal authority to act on the data subject's behalf: a written consent signed by the data subject or a certified copy of a Power of Attorney.

We may request additional information from you to help confirm the data subject's identity. We reserve the right to refuse to act on your request if We are unable to identify the data subject or verify your legal authority to act on the data subject's behalf.

IV. Information Requested

To help Us process your request quickly and efficiently, please provide as much detail as possible about the Personal Data you are requesting access to. Please include time frames, dates, names, types of documents, file numbers, or any other information to help Us locate your Personal Data.

For example, you may specify that you are seeking:

- employment records or personnel records;
- Personal Data held by a particular department;
- e-mail or other electronic communications (specify the approximate dates and times);
- billing information; and/or
- transaction histories.

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for Us to conduct a search (for example, if you request "all information about me"). We will process your access request as soon as We have verified your identity and have all of the information, We need to locate your Personal Data.

In response to your request, We will provide you with the information required by Article 15 of the GDPR, including information on:

- the purposes of processing;
- categories of Personal Data processed;
- recipients or categories of recipients who receive Personal Data from Us;
- how long We store the Personal Data, or the criteria We use to determine retention periods;

- information on the Personal Data's source if We do not collect it directly from you;
- whether We use automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing;
- your right to:
  - request correction or erasure of your Personal Data;
  - restrict or object to certain types of processing with respect to your Personal Data; and
  - lodge a complaint with our supervisory authority.

If the information you request reveals Personal Data about a third party, We will either seek that individual's consent before responding to your request, or We will redact third parties' Personal Data before responding. If We are unable to provide you with access to your Personal Data because disclosure would violate the rights and freedoms of third parties, We will notify you of this decision.

Applicable law may allow or require Us to refuse to provide you with access to some or all of the Personal Data that We hold about you, or We may have destroyed, erased, or made your Personal Data anonymous in accordance with Our record retention obligations and practices. If We cannot provide you with access to your Personal Data, We will inform you of the reasons why, subject to any legal or regulatory restrictions.

To be filled in when data subject is directly making the request:

V. Signature and Acknowledgment

I, _____, confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that: (1) [insert name of Project partner] must confirm proof of identity and may need to contact me again for further information; (2) my request will not be valid until [insert name of Project partner] receives all of the required information to process the request; and (3) I am entitled to one (1) free copy of the Personal Data I have requested, and acknowledge that for any further copies I request, [insert name of Project partner] may charge a reasonable fee based on administrative costs.

If you would like to receive a copy of the Personal Data you are requesting access to, please indicate below whether you would like a hard copy or an electronic copy:

____ Hard copy.

____ Electronic copy.

_____

Signature

_____

Date

To be filled in when the request is being made by an authorized person on behalf of a data subject:

VI. Authorized Person Signature

I, _____, confirm that I am authorized to act on behalf of the data subject. I understand that [insert name of Project partner] must confirm my identity and my legal authority to act on the data subject's behalf and may need to request additional verifying information.

_____

Signature

_____

Date

Appendix C: Retention Policy

CounteR Data Retention Period Policy

1. About this policy

The policy outlined below provides a framework for retaining Personal Data concerning data subjects in general. It is [insert name of Project Partner]'s policy to ensure that it complies with its obligations in relation to the Retention Period and erasure of Personal Data in accordance with the GDPR, LED, and all other applicable law (including National Legislation).

2. Definitions

For the Intended Purposes of this policy:

a) "**Data Protection Laws**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the "GDPR"), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data by competent authorities for the Intended Purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (the "LED") and all National Legislation.

b) "**End of Project**" mean the date upon which the CounteR Project has been officially finalised. As per the Grant Agreement, the Project's end date shall be 1st May 2023.

c) "**National Legislation**" means all National Legislation which is applicable to the Project Partner by virtue of the relevant jurisdiction.

d) "**Personal Data**" means any information relating to an identified or identifiable natural person ("Data Subject"). An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number, location data or online identifier.

e) "**Processing**" means any operation or set of operations that is performed on Personal Data, such as collection, use, storage, dissemination, and destruction.

f) "**Retention Period**" means the duration (in months or days, as applicable), which is applicable to the respective: Category/Specific of Personal Data.

This procedure only applies to Data Subjects whose Personal Data is Processed by us.

3. Determination of Retention Period Periods

Since applicable Data Protection Laws do not set out specific Retention Periods applicable to various categories of Personal Data, it is up to [insert name of PROJECT PARTNER] to determine the appropriate Retention Period in accordance with both the relevant laws and the principles of the GDPR.

The GDPR allows [insert name of PROJECT PARTNER] to hold the Personal Data for the relevant periods of time stipulated by law as a minimum. Where Personal Data is held in a manner which renders a Data Subject identifiable for a period which is longer than that stipulated by the relevant laws, that longer period must be justified by [insert name of PROJECT PARTNER]'s particular business needs. [insert name of PROJECT PARTNER] considers the following non-exhaustive list when justifying its storage of Personal Data for periods of time that are longer than the statutory periods:

a) For what is the data/information used?
b) Is [insert name of PROJECT PARTNER] subject to any legal or regulatory requirements to hold that Personal Data for a longer period?
c) Do any agreed industry practices exist in respect of that data set?
d) Is it easy or difficult to make sure it remains accurate and up to date?
e) What is the current and future value of the information?
f) What are the costs, risks and liabilities associated with retaining the information?

4. Retention Period and erasure of Personal Data

Personal Data that we Process for any Intended Purpose or Intended Purposes shall not be kept for longer than strictly necessary unless other overriding obligations oblige us hold such data for a longer period.

Our Personal Data Retention Period and erasure policy is as follows:

Category of Personal Data ("PD")	Specific PD	Retention Period ("RP")	Criterion if Infeasible to Ascertain RP
Personal Data from **social media** (pseudonymized data).	[-]	6 months from End of Project.	[-]
Personal Data from **blogs and forums** (pseudonymized data).	[-]	[-]	[-]
Personal Data from the **dark web** (pseudonymized data).	[-]	[-]	[-]
[-]	[-]	[-]	[-]

Personal Data shall be irrevocably erased and destroyed following the expiry of applicable Retention Period periods.

Appendix D: Privacy Notice Template

Privacy Notice

Version [-], last updated: [-].

This Privacy Notice ("**Notice**") applies where [Project Partner] (hereinafter referred to as the "We", "Us" or "Our") are acting as a Data Controller with respect to Our Processing of Your Personal Data for the duration of the CounteR Project, for the specific purpose(s) of the CounteR Project[16]. For more information on this Project, please visit [-].

Any Personal Data We Process is kept within Our own records in accordance with the relevant data protection and privacy laws to which We are subject including but not limited to the Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and the Law Enforcement Directive (Directive (EU) 2016/680) ("**LED**"), as may be amended from time to time (hereinafter collectively referred to as the "**Applicable Laws**").

References to "Data Controller", "Data Subject", "Personal Data", and "Process", "Processed", "Processing" in this Privacy Notice have the meanings set out in and will be interpreted in accordance with the Applicable Laws. "You" and "Your" refers to the Data Subject.

1. Data Controller Details

The Data Controller of your Personal Data is [To be Confirmed] . We are committed to respecting your privacy. If you wish to contact Us about Our privacy practices, please feel free to do so by [contacting our Data Protection Officer by] post at [-] or by email at [-]. You may also wish to contact Us by telephone on [-].

2. Personal Data

The term "Personal Data" refers to all personally identifiable information about you, directly or indirectly, and includes all the information you provide to Us or information that is provided to Us by third parties, which can be identified with you personally. The following are the Personal Data that We collect:

a) Personal Data from social media (pseudonymised Personal Data) provided by CounteR ISP – NOVA, for the purposes of Counter's research and innovation activities;
b) Personal Data from blogs and forums (pseudonymised Personal Data), also provided by NOVA for the purposes of Counter's research and innovation activities;
c) Personal Data from the dark web (pseudonymised Personal Data) that will be provided within WP3by NOVA for purpose of research and innovation activities only;
d) [-]

We [do/do not] collect and/or otherwise Process special categories of Personal Data.

Note that special categories of Personal Data include Personal Data revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric or health Personal Data, sexual orientation and Personal Data related to your conviction and offences. Typically, We do not envisage any Processing of special categories of Personal Data and as a law firm, We would only require Processing such Personal Data if We are involved in the establishment, exercise, or defence of legal claims.

When special categories of Personal Data become envisaged on another basis, We will ensure that We have additional grounds for processing Your Personal Data and will communicate to You any relevant information which may be required under applicable laws.

3. Purposes of Processing

The purposes of Processing for which your Personal Data are intended are

a) Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.
b) [-].

From time to time, We would also like to contact You about any invitation to participate in the Project's workshops, events, or other similar activities. We would also like to contact You regarding any news and updates or general information relating to the operations within the CounteR Project.

[16] *Please note that the privacy notice should be provided to the data subjects before or as soon as their Personal Data is collected.*

4. Legal Basis[17]

Our legal bases of Processing your Personal Data are:

a) Art. 6(1)(a) - (f) of the Personal Data Protection Regulation (EU) 2016/679 (the "**GDPR**").

b) Art. [-] Law Enforcement Directive (Directive (EU) 2016/680) ("**LED**").

c) Entering into and performing a contract – to provide the CounteR solution. Providing such Personal Data is necessary for developing a feasible solution against radicalisation, and counterterrorism. The consequence for not providing Us with your Personal Data would be that We would be unable to develop a solution to the issue which the Project intends to combat, and hence, will not be able to effectively achieve the abovementioned Intended Purpose.

d) Our legitimate interests – which may arise directly or indirectly in relation to the public's interest in safeguarding their vital interests, and fundamental rights under the ECHR. Whenever we process Personal Data on the basis of our, or a third party's legitimate interest, we ensure that the legitimate interest and the processing activity associated with it does not override your fundamental rights and interests relating to the protection of your Personal Data.

e) Your explicit consent – in which case, Our Processing shall be limited to the Intended Purposes specifically indicated when Your consent was requested. Processing based on Your consent is envisaged insofar as the field trials are concerned.

f) Compliance with legal obligations imposed on Us – obligations imposed on Us as a result of anti-money laundering and combating the funding of terrorism legislation, and to prevent, detect, respond, or report other potential illegal activities.

g) [-]

We may also Process your Personal Data for the purposes of establishing, exercising, or defending legal proceedings based on Our legitimate interests or compliance with legal obligations, as applicable.

5. Recipients[18]

The recipients of your Personal Data are:

a) Selected individuals from the Project Partners.

b) Law enforcement agencies.

c) Our intra-group companies and affiliates.

d) Our agents and third parties that provide services to Us; and

e) Third parties to whom disclosure may be required.

Individuals with access to your Personal Data shall be subject to the same limitations under this Privacy Notice.

6. Transfers of your Personal Data

Your Personal Data may be transferred to and stored in locations outside the European Economic Area ("**EEA**"), including to countries that may not have the same level of protection for Personal Data as provided for within the EEA. When such transfers are carried out, We will ensure that the target country has an adequate level of protection and that the transfer is lawful by putting in place the appropriate safeguards in accordance with the Applicable Laws, and/or any other applicable legislation. These appropriate safeguards include the EU Model Clauses entered into by Us and Our processors/controllers.

We may need to transfer your Personal Data in this way to fulfil a legal obligation and/or based on legitimate interests.

You can obtain more details of the protection given to your Personal Data when it is transferred outside the EEA by contacting Us using the details provided above.

7. Processing Requirement

The processing of your Personal Data is not a statutory requirement - it is a requirement for [-].

---

[17] *Lawful bases differ under the GDPR and the LED. The GDPR provides for six (6) different lawful bases (Consent, Contract, Legal Obligations, Vital Interests of Data Subject, Performance of a task carried out in public inter*

[18] *Please delete/amend as necessary. This section is intended to capture those companies/individuals who shall have access to Personal Data processed in the context of this privacy notice. The GDPR requires for there to be a written agreement in place, which agreement must satisfy a number of conditions listed within the GDPR. If context requires it, please utilise the Data Sharing Agreement Template within Appendix B*

8. Automated Decision-Making and Profiling

Your Personal Data [will/will not] be used for any automated decision-making or profiling.

9. Data Retention Period

Your Personal Data shall be held for the periods stipulated within the Table below. Thereafter, it shall be immediately and irrevocably erased unless We need to keep your Personal Data to comply with a legal obligation, or to exercise or defend any legal claim.

Type of Personal Data	Personal Data Processed	Purpose of Processing	Retention Period	Start Date
PD indicated by Project Participants s through any medium.	Name, and contact information.	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.	6 months from the end date of the Project	At the initiation of the testing phase of the Project.
PD resulting from participation of Project Partners in the development of The Project's tasks.	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.	6 months from the end date of the Project	At the initiation of the testing phase of the Project.
PD collected during field trials through the Project solution, developed within the Consortium, executed at various stages of the Project.	Photographs, audio, and/or video recordings of the participation in the Project organized activities (workshops, demonstrations, etc.)	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.	6 months from the end date of the Project	At the initiation of the testing phase of the Project.
Personal Data from **social media** (pseudonymised Personal Data)	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.	6 months from the end date of the Project	At the initiation of the testing phase of the Project.
Personal Data from **blogs and forums** (pseudonymised Personal Data)	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.	6 months from the end date of the Project	At the initiation of the testing phase of the Project.
Personal Data from **the dark web** (pseudonymised Personal Data)	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.	6 months from the end date of the Project	At the initiation of the testing phase of the Project.

10. Your Rights

For as long as We retain your Personal Data, you have certain rights in relation to your Personal Data including:

- Right of access–you have the right to ascertain the Personal Data We hold about you and to receive a copy of such Personal Data;

- Right to complain–you have the right to lodge a complaint regarding the processing of your Personal Data with the relevant supervisory authority for data protection matters;
- Right to Erasure–in certain circumstances you may request that We delete the Personal Data that we hold about You;
- Right to Object*–you have a right to object and request that We cease the processing of your Personal Data where We rely on Our, or a third party's legitimate interest for processing your Personal Data;
- Right to Portability*–you may request that We provide you with certain Personal Data which you have provided to Us in a structured, commonly used, and machine-readable format (except where such Personal Data is provided to us in hand-written format, in which case such Personal Data will be provided to you, upon your request, in such hand-written form). Where technically feasible, you may also request that we transmit such Personal Data to a third-party controller indicated by you;
- Right to Rectification–you have the right to update or correct any inaccurate Personal Data which We hold about you;
- Right to Restriction –you have the right to request that We stop using your Personal Data in certain circumstances, including if you believe that We are unlawfully processing your Personal Data or the Personal Data that We hold about you is inaccurate;
- Right to withdraw your consent–where Our processing is based on your consent. Withdrawal of your consent shall not affect the lawfulness of the processing based on your consent prior to the withdrawal of your consent; and,
- Right to be informed of the source–where the Personal Data We hold about you was not provided to Us directly by you, you may also have the right to be informed of the source from which your Personal Data originates.

Please note that your rights in relation to your Personal Data are not absolute and we may not be able to entertain such a request if we are prevented from doing so in term of an applicable law.

*The right to object against automatic decision making and the right of data portability are not present under Directive (EU) 2016/680, insofar as the processing is done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

You may exercise the rights indicated in this section by contacting Us at the details indicated above.

11. Complaints

If you have any complaints regarding Our processing of your Personal Data, we kindly ask that you please attempt to resolve any issues you may have with us first by contacting Us at the contact details included above. However, please note that you always have a right to lodge a complaint with the [-][19].

12. Processing of Personal Data relating to Minors

We may Process Personal Data relating to minors. In certain situations, this Personal Data may not be provided to Us by the minors themselves but by a third-party individual. Where this type of Processing takes place, We require that such third-party individual provides and explains this privacy notice to the minor and ensures that the minor understands the activities that are being undertaken by Us with respect to the minor's Personal Data.

By signing this Privacy Notice, you acknowledge and confirm that you have EITHER [been provided with and understood this privacy notice] OR [been provided with and explained this privacy notice to the minor in question][20]:

Signature: _____

Date: _____

[19] *Please insert details of relevant supervisory auth*

[20] *Please note the alternative options for this section. If no Personal Data pertaining to minors is collected, the second set of wording in brackets may be removed and only the wording between the first brackets should be retained. If you decide to do away with signatures all together, please also remove the beginning of this section, which states "By signing this Privacy Notice" as no signature will be collected.*

Appendix E: Informed Consent Template

[*Kindly note that it is imperative for the Controller to provide Data Subjects with their personalised Privacy Notice (Template of which may be found within Appendix [-]) before asking them to fill in the Consent Forms. In doing so, Controllers would be complying with the requirements within Articles 13 & 14 of the GDPR.*]

[Date]

Consent Form

The Data Controller responsible for processing the Personal Data for the respective purpose(s) specified below is [insert name of Project partner] with registered office at [Address]. The Data Controller is collecting your consent to process your Personal Data for the purpose of your participation in the CounteR Project.

Please tick the appropriate checkboxes if you consent to your Personal Data being processed for the abovementioned purposes, each of which are specified individually below:

Type of Personal Data	Personal Data Processed	Purpose of Processing	How Personal Data is processed	Informed Consent
PD indicated by Project Participants s through any medium.	Name, and contact information.	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.		☐
PD resulting from participation of Project Partners in the development of The Project's tasks.	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.		☐
PD collected during field trials through the Project solution, developed within the Consortium, executed at various stages of the Project.	Photographs, audio, and/or video recordings of the participation in the Project organized activities (workshops, demonstrations, etc.)	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.		☐
Personal Data from **social media** (pseudonymised Personal Data)	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.		☐
Personal Data from **blogs and forums** (pseudonymised Personal Data)	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.		☐

Personal Data from **the dark web** (pseudonymised Personal Data)	[-]	Assisting the Project in developing a feasible solution to combat radicalisation, and counter-terrorism purposes within the public's interest.		☐

Kindly tick the appropriate checkbox below and specify how you wish to be contacted accordingly.

I would like to be contacted through:

- ☐ Phone Number: _____
- ☐ E-mail address: _____
- ☐ Postal address: _____
- ☐ I would not like to be contacted.

[DC Name] is committed to protecting and respecting your privacy and will only use your Personal Data for the particular purpose(s) and processing operation(s) for which you have provided your explicit and informed consent.

You have the right to withdraw your consent at any time by [Detail Withdrawal Procedure] and contact our Data Protection Officer on [DPO Contact Details]. Such withdrawal shall not affect the lawfulness of processing based on consent obtained prior to withdrawal.

If such consent is withdrawn, it may take a reasonable amount of time to communicate such to [DC Name] to effectively stop the processing of my information. In such a case, [DC Name] will stop processing Personal Data for the purposes indicated above unless [DC Name] is otherwise required to do so for legal or compliance reasons as described in the provided Privacy Policy.

I have read and understand the information about the **CounteR** Project, as provided in the **Information Sheet** and **Privacy Notice** attached with this consent form. I understand that my participation is voluntary and I aware that I may withdraw my consent at any time. In the case of withdrawal, I understand that I shall not disclose and/or share any confidential information about the **CounteR** Project to any person.

By signing this Consent Form hereunder, you hereby acknowledge and agree that you have been provided with, read through and understood, and have no objections against our Privacy Notice, particularly section [-] which re-iterates your rights and remedies as a Data Subject.

Name: _____

Signature: _____

Date: _____

Appendix F: Data Sharing Agreement

DATA SHARING AGREEMENT

NO. [•]/ [•]

Executed by and between:

(1) [•], in its capacity as data controller ("**X**") and

(2) [•], in its capacity as data controller("**Y**");

[X] and [Y], may be referred to individually as a "Party" and collectively as the "Parties".

WHEREAS:

A. The Parties entered into the Grant Agreement no. 101021607, hereinafter referred to as 'the Grant Agreement', for the Project CounteR;
B. The Parties acknowledge that the execution of obligations under the Grant Agreement concern or include the Processing of Personal Data within the meaning of Data Protection Laws;
C. In light of this Processing, the Parties have agreed to enter into this Data Sharing Agreement ('DSA'), hereinafter referred to as the DSA, which regulates the data protection obligations of the Parties when processing the Personal Data and governs the relationship between the Parties in respect of the processing of Personal Data, and this in order to ensure compliance with the General Data Protection Regulation (GDPR) and/or other Applicable Law.

NOW THEREFORE THE PARTIES AGREE AS FOLLOWS:

2. DEFINITIONS

2.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

a) "Anonymous Data" shall mean Personal Data that has been processed in such a manner that is can no longer be attributed to an identified or identifiable natural person;
b) "Applicable Data Protection Laws" shall consist in particular of the GDPR and any other relevant data protection and privacy legislation which is applicable during the term of this Agreement, in so far as the same relates to the provisions and obligations of this Agreement, as well as any other relevant data protection and privacy legal provisions, currently in force or becoming applicable in the future, during the term of this Agreement;
c) "Authorised Employees" shall mean an Authorised Employee or contractor of either Party who has a need to know or otherwise access Personal Data to enable them to perform their obligations under this DSA;
d) "Data Protection Officer" shall mean the person nominated from time to time to hold the responsibility within each Party;
e) "EEA" shall, for the purposes of this DSA, mean the European Economic Area, United Kingdom and Switzerland;
f) "Effective Date" shall mean the effective date of this DSA, that is, the date at which this Agreement has been accepted by all the Parties;
g) "General Data Protection Regulation" or "GDPR" shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, becoming applicable from May 25th, 2018, on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive95/46/EC or any subsequent legal provision that may amend or replace such Regulation;
h) "Minimum Security Requirements" shall mean the security measures applied by the Controller's level, as detailed in Schedule 2.
i) "Processing" shall mean any operation or set of operations which is performed upon Personal Data whether or not by automatic means, including collecting, recording, organising, storing (including storage on servers located within E.U.), adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Data, as defined in the Applicable Law. The terms "Process", "Processes" and "Processed" shall be interpreted accordingly;
j) "Processing Appendix" shall mean each Schedule as set out in Schedule 1;
k) "Project Data" shall mean the Personal Data as described in a Processing Appendix together with any additional Personal Data made available within the CounteR Project and to which the Parties may have access in performing the Services;
l) "Services" shall mean the services provided by the Parties pursuant to the execution of the Grant Agreement no. 101021607 the performance of which implies the Processing of Controller Data;
m) "Special Categories of Personal Data" shall mean Personal Data which reveals:
    i. Racial or ethnic origin;
    ii. Political opinions;
    iii. Religious;
    iv. Philosophical beliefs;
    v. Trade union membership;
    vi. Genetic Data;

vii. Biometric Data;
viii. Data concerning Health;
ix. Data concerning Sex Life; and
x. Data concerning Sexual Orientation.

n) "Standard Contract Clauses" shall mean the standard contract clauses set out by the European Commission in the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 as may be amended or superseded from time to time;

o) "Supervisory Authority" shall mean the relevant supervisory authority with responsibility for privacy or data protection matters in the jurisdiction in which the Personal Data subject to this DSA is held;

p) "Technical and Organisational Measures" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, such measures being appropriate to the risks involved, which shall include Minimum Security Requirements; and

q) "Third Party" means an individual or corporate entity other than the Parties.

2.2. The terms "Data Controller", "Data Processor", "Data Subject", "Personal Data Breach" and "Consent", shall have the same meaning given to these terms in the GDPR.

2.3. References to clauses and Schedules are to the clauses and Schedules of this DSA; references to paragraphs are to paragraphs of the relevant Schedule to this DSA.

2.4. The heads given to any Clause, Schedule or paragraph shall not affect the interpretation of this DSA.

2.5. A person includes an individual, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns.

2.6. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

2.7. Words in the singular shall include the plural and vice versa.

2.8. A reference to one gender shall include a reference to the other genders.

2.9. The word "include" shall be construed to mean include without limitation.

2.10. A reference to a statute or statutory provision is a reference to it as it is in force for the time being, taking account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force made under it.

2.11. The language of this Agreement shall be the English language and for the purposes of interpretation, the provisions as they are stated in English shall be those which are considered binding.

3. APPOINTMENT

3.1. The Parties hereby acknowledge that the Project Data processed by them in connection with the performance of Services will originate from the CounteR Project.

3.2. The Parties hereby declare and warrant that they hold and will maintain valid for the entire duration of the DSA, all required approvals, consents and authorizations to Process and communicate the Project Data to the rest of the Parties. The Parties shall remain, under any circumstances, fully responsible for collecting, processing and using the Project Data.

3.3. The Parties hereby declare and warrant that, if required under the Applicable Data Protection Laws, the Parties shall inform the Data Subjects, and the relevant Supervisory Authority respectively, of the identity of any and all appointed Data Processors for Personal Data Processing operations. The Parties will be able to prove the herein appointment with this DSA.

4. DURATION

This Agreement shall commence on the Effective Date and shall continue throughout the entire duration of the Grant Agreement, which agreement covers the provision of Services between the Parties.

5. PROCESSING OF PERSONAL DATA

5.1. The Parties shall be responsible for assessing whether Personal Data can be processed lawfully and for safeguarding the rights of the Data Subjects.

5.2. The Parties warrant and undertake in respect of all Project Data that it Processes in the performance of its Services that, at all times:

a) Shall Process such Project Data only for the purposes of the CounteR Project and, in so doing, shall act solely in compliance with the Applicable Law.

b) Shall not themselves transfer, or purport to transfer, control of such Project Data to a Third Party (with the exemption of cloud storage providers whose servers are located within E.U.), except if the control/transfer is required for the fulfilment of legal obligations and/or any one of the Parties specifically instructs another Party to this effect, based on the prior consent of the Data Subject.

c) Shall keep Project Data logically separate to Data Processed on behalf of/received from any other Third Party.

d) Shall keep the confidentiality of Personal Data Processed hereunder and ensure that its Authorized Employees have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

e) Shall not Process, apply or use the Project Data for any purpose other than as required and is necessary to provide the Services.

f) Maintain and shall continue to maintain the Minimum-Security Requirements hereto attached as Schedule 2, during the term of this DSA.

g) Carry out regular tests and self-audits to ensure that the processing of Project Data it carries out conforms with the provisions of this DSA.
h) Maintain a written record of all categories of processing activities carried out its performance of its Services, containing (i) the name and contact details of the Party, any other Processors and, where applicable, the Data Protection Officer and (ii) where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organization.
i) Upon termination of the DSA, the Project Data shall, be destroyed, along with any medium or document containing Project Data.

6. DATA RETENTION

6.1. The Parties shall not retain or process any Project Data for longer than is necessary in the fulfilment of the Services.
6.2. The Parties shall destroy all the Project Data in their possession within six months of the end of the term of the Project unless a request in writing has been made by another Party for the earlier deletion of the Project Data.
6.3. Without prejudice to Clause 6.1., the Parties retain the right at law to maintain certain Project Data or any other data relating to this Agreement in accordance with any statutory or professional retention periods applicable in their respective countries and/or industry.

7. SUB-CONTRACTING

7.1. The Parties may sub-contract or outsource the Processing of Project Data under this Agreement to any other person or entity, referred to as a Data Processor, only if the first Party,
a) has provided reasonable prior notice to the rest of the Parties of the identity and location of the Data Processor and a description of the intended Processing to be sub-contracted or outsourced to the Data Processor to enable the other Parties to evaluate any potential risks to Project Data.
b) has imposed legally binding contract terms substantially the same as those contained in this Agreement on the Sub-Processor including, if appropriate, the Transfer Contract Clauses ("Data Processor Contract"); and
c) The other Party has been informed, understands and agrees to the storage of data by the Data Processor.

8. SECURITY OF COMMUNICATIONS BETWEEN THE PARTIES

8.1. The Parties shall undertake technical and organisational measures to safeguard the security of any electronic communications, if used for the purpose of this DSA, to transfer or transmit Project Data (including but not limited to measures designed to ensure the secrecy of communications and prevent unlawful surveillance or interception of communications and gaining unauthorised access to any computer or system and thus guaranteeing the security of the communications), which measures are listed in Schedule 2 of this DSA.
8.2. The Parties shall keep the Project Data logically separate to Personal Data processed on behalf of any other Third Party or its own behalf.

9. NOTIFICATIONS

9.1. Any notice, letter or other communication contemplated by this Agreement shall be made in writing and addressed to the Parties using the following contact details:
[•]

10. EXERCISE OF DATA SUBJECTS' RIGHTS

10.1. Any Data Subject request received directly by the Parties shall be handled by each Party in accordance with Applicable Data Protection Laws.
10.2. The Parties shall assist each other, insofar as this is possible, for the fulfilment of its obligation to respond to requests for the exercise of the Data Subject's rights.

11. NOTIFICATION OF PERSONAL DATA BREACHES

11.1. The Parties shall notify each other of any Personal Data Breach not later than 24 (twenty-four) hours after having become aware of such breach. The notification shall be accompanied by any necessary documentation to enable the Parties, to contain the Personal Data Breach.
11.2. Such notification shall include:
a) a detailed description of the Personal Data Breach;
b) the type of data that was the subject of the Personal Data Breach;
c) the identity of each affected person (or, where not possible, the approximate number of Data Subjects and of Personal Data records concerned);
d) the name and contact details of the Party's Data Protection Officer or Representative, where applicable, or any other point of contact where more information can be obtained;
e) a description of the likely consequences of the Personal Data Breach;
f) a description of the measures taken or proposed to be taken by the Party to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

11.3. In addition, each Party affected shall, where necessary, notify the Personal Data Breach to the relevant Supervisory Authority and/or the Data Subjects in question.

12. DOCUMENTATION

The Parties shall provide each other, upon written request, with the necessary documentation in order to demonstrate that the Processing is compliant with the Applicable Data Protection Laws and this DSA.

13. APPLICABLE LAW

13.1. This Data Sharing Agreement shall be construed in accordance with and governed by the laws of [-].
13.2. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State. The Parties agree that those shall be the courts of _____ (specify Member State).

14. MISCELLANEOUS

14.1. As part of their contractual relations, the Parties hereby undertake to comply with the applicable regulations on Personal Data processing and, in addition, shall agree to the Consortium Code of Ethics as found on [insert link].
14.2. This Agreement, including the Schedules attached hereto and any subsequent, properly executed Processing Appendices agreed between the Parties, constitute the entire agreement between the Parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations and discussions between the Parties.
14.3. The provisions of this Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this Agreement shall remain in full force and effect.
14.4. The provisions of this Agreement shall endure to the benefit of and shall be binding upon the Parties and their respective successors and assigns.
14.5. This Agreement may be executed in counterparts, each of which, after signature and dispatch, shall be deemed an original, but all of which together shall constitute one and the same instrument.

IN WITNESS THEREOF, this Agreement was executed and signed in [X] original copies in English, one original copy for each contracting Party.

Schedule 1 to the Data Sharing Agreement dated [•]/ [•] - Processing Appendix

Data subjects:

[•]

Categories of data:

[•]

Special categories of data (if appropriate):

[•]

Processing operations/ nature of operations carried out on the data:

[•]

Transmission/ Transfer of data:

[List of relevant non-EU States] and EU Member State

Schedule 2 to the Data Sharing Agreement [•]/ [•] - Minimum Security Requirements

[The Security Requirements to be followed by the Parties shall be attached to this Agreement.]

Note that the formal Security Requirements are still under development. The list below is to serve as a high-level guidance note which is aimed at streamlining one's thought process as to how the Software Development Life Cycle ("**SDLC**") is to be handled from a data protection perspective.

Furthermore, the below is to be consulted on a case-by-case basis, depending on the respective Project Partner's resources, and the technical feasibility of implementing the CounteR solution.

1. Risk Assessment
2. Security Policy
3. Organisation of Information Security
4. Asset Management

5. Human Resources Security
6. Physical & Environmental Security
7. Communications & Operations Management
8. Access Management
9. Information Systems Acquisition, Development & Maintenance.
10. Business Continuity Management
11. Compliance.

Appendix H: Legitimate Interest Assessment Template

The present Legitimate Interest Assessment ("**LIA**") is to be used by [insert name of Project Partner] in order to assess whether [insert name of Project Partner] may process Personal Data in reliance on article 6(1)(f) of the GDPR. The purpose of this LIA is to assess whether the processing of Personal Data in the manner intended by [insert name of Project Partner] overrides 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. In making such an assessment, [insert name of Project Partner] shall pay particular attention to the questions posed within this LIA.

Part 1: Purpose Test

[*Here, one must assess whether there is, in fact, a legitimate interest behind the Project. Processing should be in done in a manner which reaches pre-defined goal or an '**end-result**', which must be circulated to Data Subjects.*]

What is the legitimate interest being pursued by [insert name of Project Partner]?

- Why does [insert name of Project Partner] want to process the data?
- Does [insert name of Project Partner] need to process the data?
- What benefit or benefits does [insert name of Project Partner] expect to get from the processing?
- Will any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if [insert name of Project Partner] could not go ahead with the processing?
- Is [insert name of Project Partner] complying with any specific data protection rules that apply to its processing?
- Is [insert name of Project Partner] complying with other relevant laws?
- Is [insert name of Project Partner] complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

Part 2: Necessity Test

[*Here, one must assess whether the Project is strictly necessary for the purpose you have identified above. Kindly note that necessity must be established in relation to the specific purpose, and not as a catch-all.*]

[insert name of Project Partner] needs to assess whether the processing is necessary for the purpose(s) [insert name of Project Partner] has identified.

- Will this processing actually help [insert name of Project Partner] achieve its purpose(s)?

• Is the processing proportionate to that purpose? • Can [insert name of Project Partner] achieve the same purpose(s) without the processing? • Can [insert name of Project Partner] achieve the same purpose(s) by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

[*Here, one must consider the impact that the Project may have on the individual's interests, rights, and freedoms. Furthermore, an assessment must be conducted to ascertain whether these overrides the Data Subject's legitimate interests.*]

[insert name of Project Partner] shall assess whether the legitimate interest(s) set out in Part 1 and the necessity in Part 2 override the data subjects' interests, rights and freedoms.

Nature of the Personal Data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Is [insert name of Project Partner] processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?

Reasonable expectations
• Does [insert name of Project Partner] have an existing relationship with the individual? • What's the nature of the relationship and how has [insert name of Project Partner] used data in the past? • Did [insert name of Project Partner] collect the data directly from the individual? What did [insert name of Project Partner] tell them at the time? • If [insert name of Project Partner] obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover [insert name of Project Partner]? • How long ago did [insert name of Project Partner] collect the data? Are there any changes in technology or context since then that would affect expectations? • Is [insert name of Project Partner] intended purpose and method widely understood? • Is [insert name of Project Partner] intending to do anything new or innovative? • Does [insert name of Project Partner] have any evidence about expectations – e.g., from market research, focus groups or other forms of consultation? • Are there any other factors in the particular circumstances that mean they would or would not expect the processing?
Likely impact

• What are the possible impacts of the processing on people? • Will individuals lose any control over the use of their Personal Data? • What is the likelihood and severity of any potential impact? • Are some people likely to object to the processing or find it intrusive? • Would [insert name of Project Partner] be happy to explain the processing to individuals? • Can [insert name of Project Partner] adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

4. Outcome of LIA

Is a Data Protection Impact Assessment required?	Yes/No
Can [insert name of Project Partner] rely on legitimate interests for this processing?	Yes / No
Does [insert name of Project Partner] have any comments to justify its answer? (optional)	
LIA completed by	

Date	
DPO Signature (if applicable)	

This LIA shall be kept under review and shall be reviewed every [*insert period of time after which the LIA will be reviewed*].