PROPHETS

Preventing Radicalisation Online through the Proliferation of Harmonised Toolkits

H2020 - 786894

D2.5 Project Ethical and Legal Handbook

Lead Author: Sarina Ronert, Stephanie Stangl (BayHföD)
With contributions from: Jürgen Teubert (BayHföD)
Reviewer: Dimitris Kavallieros (KEMEA), Sara Gambino (TVD)

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	28th February 2019
Actual delivery date:	18th February 2019
Version:	1.0
Total number of pages:	24
Keywords:	Ethics, Data Protection, Templates, Handbook

Abstract

This document is intended to provide an overview about the meaning of 'ethics' and data protection, how these relate specifically to the PROPHETS project and what partners must do in order to comply with the respective requirements.

Executive summary

As our research and outputs involve and have an impact on human beings, we have to determine whether anything we do as a project is capable of having a negative impact on those it involves. It should be ensured that approaches, methods, outputs and dissemination activities demonstrate the ethical and legal principles worked out within this deliverable. The following actions in respect of PROPHETS activities should be carried out for each phase of development or research activity:

- **Identify a Data Protection Officer or representative** - this can either be an organizational / formal DPO or, if the organisation does not have one, a person who will take on this role for the purposes of the project and act as a single point of contact, as well as providing assurances about compliance, using the forms provided.
- **Provide a declaration of data protection compliance on behalf of your organisation** – this can be a declaration by the DPO / representative or a copy of approval from the national supervisory authority, if this is required. A form accompanies this document.
- **Identify the legal foundation for all data processing** – this may vary, depending on the nature, purpose and context of the activity. It must be established before any processing begins. Note this along with the associated records for the data processing (template 6).
- **Provide confirmation and details of security measures** – that will be applied to personal data being processed for any purpose within the PROPHETS project (template 6).
- **Complete risk assessment checklist** – for all data processing activities carried out within the PROPHETS project (template 4).
- **Carry out data protection impact assessments (DPIA)** – for all data processing activities identified as having a degree of risk for data subjects either individually or as a group (template 5). Special categories of personal data pursuant to article 9 GDPR in principle are not collected or processed.
- **Use consent forms and information sheets** – for all activities where the legal basis for data processing is consent. The templates provided here should be adapted to the specific nature, purpose and context of the activity (information sheet: template 1); (consent form: template 2).
- **Keep records of data processing** – this includes consent forms, information sheets, dates, times, purpose of processing, legal foundation, risk assessments, security measures, rationale for decisions. This information will be requested (template 6).
- **Use the ethics checklist** (template 3) to identify any risks arising from new work or research activities. If risks are identified then a risk assessment should be carried out. The checklist should be kept with the research / development paperwork.
- **Include copies of all** ethics and data management documents in deliverables reporting research, as annexes, this includes consent and information sheets, risk assessments, methods of selecting participants and data management plan.

Document Information

IST Project Number	786894	**Acronym**	PROPHETS
Full Title	Preventing Radicalisation Online through the Proliferation of Harmonised Toolkits		
Project URL	www.prophets-h2020.eu		
EU Project Officer	Laure Guille		

Deliverable	**Number**	D2.5	**Title**	Project legal and ethical handbook
Work Package	**Number**	WP2	**Title**	Legal, Political and Ethical Aspects of Online Behavioural Radicalisation

Date of Delivery	**Contractual**	M10	**Actual**	M10
Status	version 1.0		final	
Nature	report			
Dissemination level	public			

Authors (Partner)	Hochschule für den öffentlichen Dienst in Bayern – Fachbereich Polizei			
Responsible Author	**Name**	Sarina Ronert (BayHföD)	**E-mail**	Sarina.ronert@pol.hfoed.bayern.de
	Partner	BayHföD	**Phone**	0049 8141 408 232

Abstract (for dissemination)	This document is intended to provide an overview about the meaning of 'ethics' and data protection, how these relate specifically to the PROPHETS project and what partners must do in order to comply with the respective requirements.
Keywords	Ethics, Data Protection, Templates, Handbook

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
07.01.2019	0.1	Sarina Ronert, Stephanie Stangl	Main structure and initial draft
09.01. – 01.02.2019	0.2	Sarina Ronert, Stephanie Stangl	Edit and development
21.01 – 08.02.2019	0.3	Jürgen Teubert	Development
08.02. – 11.02.2019	0.4	Sarina Ronert, Stephanie Stangl	Development
12.02. – 18.02.2019	0.5	Sara Gambino, Dimitris Kavallieros	Review
18.02.2019	1.0	Sarina Ronert, Stephanie Stangl	Finalisation

Table of Contents

Abbreviations

ALLEA: All European Academies

DPO: Data Protection Officer

DPIA: Data Protection Impact Assessments

GDPR: General Data Protection Regulation

LEA: Law Enforcement Agency

1 Introduction

This document is intended to provide an overview about the meaning of 'ethics' and data protection, how these relate specifically to the PROPHETS project and what partners must do in order to comply with the respective requirements.

Even though there are data protection and human rights laws to protect individuals, ethics laws' as such do not exist. Therefore, it is the responsibility of each project partner to carry out their tasks in a way that incorporates respect and protection of human values. Ethical principles are context specific in most cases, wherefore the most relevant to the PROPHETS project are presented in this handbook. The standards pertaining to Horizon 2020 projects and the ALLEA (All European Academies) Code of Conduct for Research Integrity remain the core considerations:

It must be emphasised here and elsewhere that compliance with data protection law in every area of the PROPHETS project is of the utmost importance and is every partner's responsibility.

The term 'Data Protection by Design and by Default' refers to a concept in which data protection and privacy are integral to what we do, meaning that these considerations and corresponding actions are at the forefront, not 'bolted on' at the end or included as an afterthought. In particular, the 'Data Protection by Design' approach means that the whole team focuses on the issues and risks from the outset and they are interwoven throughout everything thereafter. We must avoid creating unnecessary or disproportionate risk to individuals, whose data we process, through our work.

The actions and guidance described in this guide are done so within the context of the PROPHETS project, so that we can demonstrate our compliance with legal and ethical requirements. Nothing in this guide is intended to alter or supersede any existing legal obligations that partners have or any professional and organisational principles/practices that apply to PROPHETS partners. Nor is the content intended as legal advice but merely guidance, so that the PROPHETS project can achieve its stated outcomes in a way that demonstrates integrity, social responsibility and lawfulness.

2 What do we mean with "Ethics"?

Research ethics can be described as a set of standards that affords protection to all those involved in the research, whilst maximising the value and benefits of the endeavour. The standards apply to researchers planning, carrying out and disseminating research and require them to adhere to certain principles. The ALLEA Code of Conduct for Research Integrity emphasises the responsibility of individuals and organisations carrying out the research to align with the principles of honesty, integrity, accountability and respect.[1]

2.1 Principles

- **Reliability:**
  Includes validating information and sources. Use of recognized methods and analyses. Justify decisions and actions with underlying rationale.
- **Honesty:**
  About limitations of methods or outcomes. Accurate reporting of findings. Correct omissions, misuse of data and avoid misleading outputs. Report wrongdoing appropriately.
- **Respect:**
  For the rights of participants and others affected by research. Personal data and confidential information should be safeguarded appropriately. Equality for all (e.g. gender), should be integrated.
- **Accountability:**
  Each researcher should take responsibility for complying with ethical standards and principles at every stage of the activity. Records should be made and kept to demonstrate this. Ensure appropriate use of public funding.
- **Integrity:**
  Incorporate scientifically sound practices, rigorous methods and quality data. Objective analysis of evidence. Impartiality and freedom from pressures or conflicts of interest. Compliance with all relevant legal and ethical requirements.
- **Transparency:**
  About the purpose, methods and planned uses of the research. Provide publicly available outcomes, where possible. Openness about assumptions, findings and conclusions.
- **Minimise harm & maximise benefit:**
  Includes emotional, mental, physical, financial and social standing of any involved person. Includes stigmatization of individuals / groups or consequences that could be perceived as discriminatory.
- **Excellence:**
  Ethics approvals should be obtained prior to activities that pose significant risks. Researchers should have professional competency. Aim to produce work of the highest quality.
- **Fairness:**
  Acknowledge the contribution of others and accurately reference others' work. Ensure no individual group is disadvantaged or unfairly represented.

[1] ALLEA (2017): The European Code of Conduct for Research Integrity. Revised Edition. Berlin (http://www.allea.org/wp-content/uploads/2017/03/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017-1.pdf)

2.2 How does this relate to PROPHETS?

The value of innovations in technology, new tools and different approaches to problems are enormous and it is undeniable that they can benefit society in numerous ways. However, there are also serious concerns about the related impact on human rights and ethical issues. This calls for new approaches to minimise the potential risks and focus efforts on incorporating ethical considerations.

As researchers and developers of innovative technology, each member of the PROPHETS project bears a responsibility to ensure that any negative impacts of their work and the outputs are identified and minimised, so that the benefits are not at the expense of rights and freedoms but complement and respect them.

Some of the PROPHETS research and development work may be inherently risky, due to the subject matter and the nature of the PROPHETS solution. Some of these are outlined below.

- **Development and testing of new technology:**
  Automated systems have the potential to remove the element of human discretion and therefore control. Automated decision-making / profiling is inherently high risk due to the lack of control of those involved. Assumptions may be made about individuals by combining datasets and sources; unfairness or discrimination may result.

- **Large-scale data collection:**
  Data subjects are unknown and may include vulnerable people and children; lack of control over the content of the data; potential intrusion on individuals' rights and freedoms etc.

- **Individuals unaware of actions**:
  Those whose data is being collected are unaware of this and therefore cannot easily exercise their rights; it is unlikely that data subjects would expect their data to be processed in this way, which is different to the purpose for which it was posted by them.

- **Cross-border research:**
  Drawing data from open sources will inevitably involve data subjects from different countries, including outside the EU. This may raise different legal and ethical issues.

- **Collection of disturbing content:**
  It is possible that, due to the nature and subject matter of the project, researchers and testing participants can be exposed to distressing images and content.

- **Nature of information:**
  It is possible that during testing and development, incidental findings will occur, that may create an ethical dilemma or require further action.

- **Potential misuse:**
  Due to the nature of the material collected, the potential impact of misuse of data could be serious.

3 Data Protection Overview

Privacy, closely related to data protection but remaining distinct, has been a fundamental right not only for EU citizens but globally for 70 years. First set out in the United Nations Declaration of Human Rights in 1948 and incorporated into the European Council's European Convention on Human Rights in 1950, this fundamental human right is the source of data protection law as it continues to develop in order to remain relevant and effective with the evolution of society. The European Council furthered its aims with Convention 108 in 1981, which inspired the European Union's Data Protection Directive in 1995.

Data protection is also now a fundamental right for European citizens; this is enshrined in the EU Charter of Fundamental Rights, which achieved Treaty status in 2009, under the Lisbon Treaty, meaning that this applies to all citizens in all Member States directly.

The most recent embodiment of these fundamental rights is the General Data Protection Regulation (GDPR-Regulation (EU) 2016/679), which came into effect across Europe in 2018. Most countries across the globe have developed or are developing legislation that aligns with European standards.

The current focus on data protection issues is due to the evolution of the digital age; more advanced technological capabilities, combined with a greater number of people engaging with online activities, means that some fundamental rights are exposed to greater risks of violation, in particular privacy and data protection. Although it is beyond doubt that the digital age provides greater opportunities and benefits for all sections of society, it also provides the opportunity for rights to be more easily violated. The data protection laws seek to pave a way where all people can share benefits, without compromising fundamental rights.

3.1 What does the GDPR say?

The purpose of the GDPR is to make the protection of fundamental rights and freedoms relevant and effective in the digital age. This is because the risks, certainly relating to data protection and privacy, are much greater due to so much personal information being put online in 'public' spaces.

This means that people have much less control over what happens to their data and allows people and organisations to use, process and even manipulate that personal information to their own advantage, often to the individual's detriment and often without their knowledge.

The GDPR increases the responsibilities and obligations of the data controller and strengthens the rights of the individual data subject. Individuals should have a clear understanding of exactly what is happening to their personal data and be allowed to exercise their various rights in relation to it.

3.1.1 Definitions (See Article 4 GDPR)

Some of the terms that are most relevant in the context of PROPHETS.

- **Personal Data** - *any information relating to an identified or identifiable natural person (data subject) […] 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;*
- **Special Categories of Personal Data** - *[…] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation […]*
- **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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,*

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **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; […]*
- **Data Processor** - *means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*
- **Profiling** - *means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*

3.1.2 Data Protection Principles

In addition to the specific requirements set out in the GDPR, there are seven overriding principles that must form the core considerations of all activities involving the processing of personal data.

- **Lawfulness, Fairness and Transparency**
  Any processing of personal data must be lawful and fair. It should only be carried out if the purpose of the processing could not be achieved by other means.

- **Purpose Limitation**
  Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the first.

- **Data Minimization**
  The personal data must be adequate, relevant and limited to what is necessary to achieve the purpose for which they are processed.

- **Accuracy**
  Every reasonable step must be taken to ensure that personal data being processed are accurate, relevant and where necessary kept up to date, having regard to the purposes for which they are processed. Where required, they must be erased or rectified without delay.

- **Storage Limitation**
  Not kept longer than necessary for the purposes for which it was processed.

- **Integrity and Confidentiality**
  Processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

- **Accountability**
  The controller is responsible for, and able to demonstrate, compliance with the GDPR requirements.

3.1.3 Privacy Rights of those affected (see Article 12 et seq. GDPR)

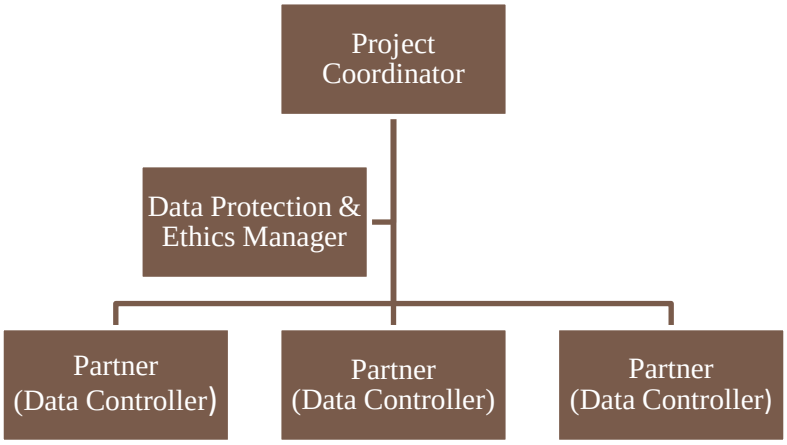
Some of the terms that are most relevant in the context of PROPHETS:

- Duty to inform when collecting information from the person affected (e.g. on the web page)
- Right to information
- Right to rectification and cancellation
- Right of objection in case of processing due to balance of interests and revocation of consent
- Right to fundamentally non-automated decision-making in individual cases (see article 22 GDPR)
- Right to data portability
- Restriction options
- Appeal possibility to the supervisory authorities

3.2 How does this relate to PROPHETS?

Within the PROPHETS project, there are several partners who will process personal data of various kinds, from various sources, during their research, development and testing work. Because each one of these partners is making their own decisions about which personal data to process and how to process it, they will each be a data controller in their own right. However, due to each of these data controllers being part of a single project, with a single aim, then the project as a whole is made up of joint controllers. Each one is individually responsible for their compliance.

Organisation of data protection responsibilities within PROPHETS



Additionally, every member of the project consortium has a personal responsibility to carry out their tasks in a way that ensures data protection compliance. This structure and putting data protection at the forefront of considerations demonstrates a Data Protection by Design and by Default[2] approach by the project.

There are three main areas in the project that may involve processing personal data:

1. Processing personal data during ‘every day’ activities as a PROPHETS partner, for example:
    a. Communicating with other consortium members or those associated with the project;
    b. Carrying out dissemination activities;
    c. Sharing research / development / testing outcomes with partners or wider.

2. Carrying out development work using personal data from various sources;

[2] GDPR, Article 25.

3. Carrying out testing activities involving individuals, who are either internal or external to the project.

Please note - law enforcement authorities who are carrying out research, development or testing within PROPHETS are doing so for research purposes, not law enforcement purposes. Therefore, the GDPR applies to their activities rather than the Law Enforcement Directive (DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016).

Essential data protection principles for the PROPHETS project

- Compliance with data protection rules and principles must be demonstrated (see Note 1. below).
- By anonymization or pseudonymization of the data collected, any conclusion on subjects or radicalized persons is to be prevented (see Note 2. below).
- The principle of transparency is fulfilled (see Note 3. below).

1. Usually, data controllers are obliged to inform individuals about this process and the criteria used to make decisions or categorise them. Security measures must be implemented and close adherence to the data protection rules and principles must be demonstrated. It is intended to comply with EU rules, and thus also Articles 15, 16, 18 and 21 GDPR. The participants are informed in an information sheet and a declaration of consent, among other things, that the participation takes place voluntarily and can be terminated at any time without giving reasons. Also, individual questions of the questionnaire can remain unanswered. In addition, data subjects are given the right to be informed about the purpose of the collection, use of data, storage and retention of the data provided.

2. The survey data concern own experiences for the radicalization of other persons as well as the procedure of the radicalization processes. In principle, the data collected is stored in anonymised or pseudonymised form. A personal assignment neither to the subject concerned nor to the radicalized person is not possible and technically impossible. If the questionnaire contains free-text entry fields for the survey, there is the possibility of a personal assignment depending on the content of the entry. Therefore, the information in free-text input fields on a voluntary basis. This is explicitly indicated in the questionnaire. The survey is carried out by means of predefined questionnaires manually or online. Insofar as IP-addresses of the test persons are collected in the online survey method, these are to be anonymised, so that it is not possible to draw any conclusions about the subject's person via the provider. Special categories of personal data pursuant to article 9 GDPR are not collected or processed.

3. The principle of transparency presupposes that all information and communications on the processing of such personal data are accessible, understandable and in clear and simple language. This principle concerns, in particular, the information on the identity of the person responsible and the purposes of the processing and any other information which ensures fair and transparent processing with regard to the natural persons concerned, as well as their right to obtain confirmation and information as to which they concern personal data is processed. The requirements on the transparency of the information, the communication and the modalities for the exercise of the rights of the data subject pursuant to article 12 GDPR are complied with.

4 What do I need to do?

As our research and outputs involve and have an impact on human beings, we have to step out of our committed expert role and adopt a different perspective in order to determine whether anything we do as a project is capable of having a negative impact on those it involves. This includes researchers, participants, organisations, LEAs / end-users and wider society.

We can not only navigate and minimise the risks, but by confronting and addressing these risks we can also show that innovative LEA methods can benefit end-users and protect people. To ensure transparency, we need policies, practices and procedures in place. It should be guaranteed that approaches, methods, outputs and dissemination activities demonstrate the ethical principles referred to above.

Also, the important things to remember are the overriding principles and aims of the legislation. It is a risk-based approach, based on individual's rights and freedoms. Furthermore, it is a balancing act so that we achieve our legitimate aims with minimal impact on the individuals involved during our project activities.

The below actions relate to requirements for the PROPHETS project specifically, they do not alter or supersede any ordinary obligations and responsibilities imposed by data protection law. If consortium members intend to involve participants into project activities (i.e. testing of the platform or focus groups), they need to ensure that each participant signs template 1 (information sheet) and template 2 (consent form). Moreover, for every planned research activity, partners need to use the ethics checklist (template 3), whereas all data processing activities need a completed risk assessment checklist (template 4). In the case either of the templates indicates that further measures are required, template 5 (data protection impact assessment) and template 6 (records of data processing) must be applied. All partners are responsible to collect and keep on file all respective documents up to three years after the end of the project. Additionally, a copy of each document must be sent to the coordinator.

- **Identify a Data Protection Officer or representative** - this can either be an organizational / formal DPO or, if the organisation does not have one, a person who will take on this role for the purposes of the project and act as a single point of contact, as well as providing assurances about compliance, using the forms provided.
- **Provide a declaration of data protection compliance on behalf of your organisation** – this can be a declaration by the DPO / representative or a copy of approval from the national supervisory authority, if this is required. A form accompanies this document.
- **Identify the legal foundation for all data processing** – this may vary, depending on the nature, purpose and context of the activity. It must be established before any processing begins. Note this along with the associated records for the data processing (template 6).
- **Provide confirmation and details of security measures** – that will be applied to personal data being processed for any purpose within the PROPHETS project (template 6).
- **Complete risk assessment checklist** – for all data processing activities carried out within the PROPHETS project (template 4).
- **Carry out data protection impact assessments (DPIA)** – for all data processing activities identified as having a degree of risk for data subjects either individually or as a group (template 5). Special categories of personal data pursuant to article 9 GDPR in principle are not collected or processed.
- **Use consent forms and information sheets** – for all activities where the legal basis for data processing is consent. The templates provided here should be adapted to the specific nature, purpose and context of the activity (information sheet: template 1); (consent form: template 2).
- **Keep records of data processing** – this includes consent forms, information sheets, dates, times, purpose of processing, legal foundation, risk assessments, security measures, rationale for decisions. This information will be requested (template 6).

- **Use the ethics checklist** (template 3) to identify any risks arising from new work or research activities. If risks are identified then a risk assessment should be carried out. The checklist should be kept with the research / development paperwork.
- **Include copies of all** ethics and data management documents in deliverables reporting research, as annexes, this includes consent and information sheets, risk assessments, methods of selecting participants and data management plan.

A data protection by design and by default culture must be maintained; data protection matters must be at the forefront of considerations before commencing any research, development or testing and must be demonstrated. This should be the gateway; if compliance is not achieved then the work cannot be carried out. Before each task or activity, consider the questions set out below:

What is the purpose of the activity?	➢ What needs to be achieved?
Does personal data need to be processed?	➢ Is it necessary? ➢ Is there another way?
What is the legal basis?	➢ Consent? (freely given, informed) ➢ Public interest? (national law req'd) ➢ Legitimate interest? (justify, explain) ➢ Consider all relevant bases
How much personal data is needed?	➢ Minimum to achieve the purpose ➢ Proportionate and necessary
What are the risks to the data subjects?	➢ Screening questions ➢ Data Protection Impact Assessment ➢ Mitigate risks / consult / report
Are appropriate security measures in place?	➢ Consider resources & severity of risk ➢ Technical and organisational
Does the personal data need to be retained?	➢ What security measures required? ➢ Minimum amount for minimum time ➢ Review and justify retention periods
Will the personal data be shared?	➢ Recipient standards must align ➢ Minimum necessary for the purpose
Will the data be used for a further purpose?	➢ Consider anonymization ➢ Compatibility test (linked purpose) ➢ New legal basis if different purpose

Annex A Template 1 – Information Sheet

INFORMATION SHEET
FOR PARTICIPANTS IN ACTIVITIES TO SUPPORT THE PROPHETS PROJECT

The Project

PROPHETS (Preventing Radicalisation Online through the Proliferation of Harmonised ToolkitS) will look at redefining new methods to prevent, investigate and mitigate cybercriminal behaviours through the development of a coherent, EU-wide, adaptive SECURITY MODEL, built upon the interplay of the human factors within the new cyber ecosystem and capable of addressing the four fundamental dimensions at the core of the phenomenon:

1. early identification of security threats;
2. investigations within a new public-private governance;
3. Increased complexity of the response due to the expansion of the security perimeter towards new societal fields and the emergence of challenging jurisdictional problems; and, last but not least,
4. perception of security and freedoms among citizens, which requires a new communication strategy for LEAs and security policy

Your participation

The activity described below is being carried out as part of the PROPHETS project and your participation is valuable to help us do this. We would like to collect and process some of your personal information for this purpose but we can only do this with your freely given consent, which is the legal basis for this processing. You can consent to only some of your information being used by checking the appropriate boxes on the consent form.

We will not process any of your information if you do not give your consent, or if you change your mind; you can withdraw your consent at any time during or after the activity by using the contacts given at the end of this document.

We will only collect and process the minimum amount of information that is required to achieve the purpose stated below. We will apply appropriate security measures during all processing and storage of your data; these are described below. You have rights in respect of your personal data, which we fully respect and comply with; these are also described below.

The activity

The survey data concern own experiences for the radicalization of other persons as well as the procedure of the radicalization processes. In principle, the data collected is stored in anonymised or pseudonymised form. A personal assignment neither to the subject concerned nor to the radicalized person is not possible and technically impossible.

Will the personal data be shared?

A data transmission does not take place.

Will the personal data be stored?

The collected data is stored in each state of the state involved in the project on its own responsibility. The data collected by the research institute of the BayHfoD are stored on servers of the BayHfoD. The data collected by the participating States will be transmitted to the coordinating participant. The coordination of this project is the responsibility of the BayHfoD. Data backups take place within the scope and scope of the BayHfoD.
The members of the research institute of the BayHfoD as well as the members of the system administration of the BayHfoD have access to the stored data as part of their function. The access to the server room is only up to the members of the system administration of the BayHfoD.
The collected data will be stored for the duration of the project (36 months from project start on 01.05.2018). These data will be stored for the purpose of an audit for a further three years after completion of the project. Thereafter, the data is not reconstructed from all storage media deleted.
A profiling within the meaning of article 4 GDPR- Regulation (EU) 2016/679 does not take place.

Your rights

- You can request access to your data, or amend it, or delete it at any time
- You can withdraw consent for any part, or all, of the data processing
- Some questions in the questionnaire can go unanswered.
- You will be informed about the purpose of the collection, the use of the data, storage and storage of the provided data.
- You can request that we transfer your personal data to another organization
- You can lodge a complaint with the data protection supervisory authority

Contact details

- National data protection supervisory authority: Bayerischer Landesbeauftragter für den Datenschutz, Prof. Dr. Thomas Petri, Postfach 22 12 19, 80502 München
- PROPHETS Project Coordinator: Dr. Holger Nitsch, holger.nitsch@pol.hfoed.bayern.de
- PROPHETS Ethics & Data Protection Manager: Jürgen Teubert, juergen.teubert@pol.hfoed.bayern.de
- Data Protection Representative for this activity: Jürgen Teubert, juergen.teubert@pol.hfoed.bayern.de
- Facilitator / Researcher for this activity:

Annex B Template 2 – Consent Form

Consent Form
PROPHETS

Please respond to the following statements by ticking the response that applies.

	Yes	No
1. I have read the Information Sheet for this study and have had details of the data processing explained to me.	☐	☐
2. My questions about what will happen to my personal data have been answered to my satisfaction and I understand that I may ask further questions at any point.	☐	☐
3. I understand what I am being asked to do and agree to being involved in this research activity.	☐	☐
4. I understand that I can withdraw my consent at any time and how to do this.	☐	☐
5. I understand my rights in relation to my personal data as set out on the Participant Information sheet, and how to exercise them.	☐	☐
6. I have been provided with a copy of the information sheet about this activity, which includes details of people to contact if I need to.	☐	☐
7. I agree to my personal data being securely retained by the research team only, for them to contact me in the future about this or related research activities.	☐	☐
8. I consent to the processing of my personal contact details for the purposes of this activity, which is limited in the way described in the Participant Information sheet.	☐	☐
9. I consent to the information collected for the purposes of this research study, once anonymised (so that I cannot be identified), to be used for any other research purposes.	☐	☐

Thank you. Please sign overleaf.

With my signature, I declare my agreement to the above-mentioned contents:

Signed: …….. **Name**: ……

Date: ……/……/……..

Researcher / Facilitator's Statement: I ……. (name) confirm that I have carefully explained the nature, demands and foreseeable risks of participating in the activities for the PROPHETS project to the volunteer. I understand my role as data controller for any data provided by the contributor.

Signed: …….. **Name:** ……..

Date: ……/……./…….

Please keep your copy of the consent form and the information sheet together.

Annex C Template 3 – Ethics Check List

ETHICS CHECK-LIST

No.	Question	Yes	No
1.	Does the proposed activity involve the use of human participants?		
2.	If 'yes', would they be considered to be potentially vulnerable?		
3.	Will the activity involve the collection of confidential or sensitive information?		
4.	Will the activity involve controversial subject matter?		
5.	Will the activity expose researchers, participants or others to harm of any kind?		
****If the answers above are 'No' then no formal approval is necessary ****			
5.	Has the activity already received approval from an ethics committee?		
6.	Is the activity part of a larger study, which has already received approval from an ethics committee?		
**** If answer to either 5 or 6 is 'Yes' then no further approval is necessary ****			
7.	Have considerations to health and safety risks posed by the activity been made?		
8.	Are data protection compliance measures in place for any personal data collected by the activity?		

Annex D Template 4 – Risk Assessment Check List

RISK ASSESSMENT CHECK-LIST

The risk assessment questions serve to identify any possibility of risk arising from the planned activity. If the outcome indicates no risk then no additional action, other than ordinary compliance measures, needs to be taken. If any questions are answered 'yes' then a full data protection risk assessment **must** be carried out.

No.	Question	Yes	No
1.	Does the activity involve systematically monitoring publicly accessible spaces?		
2.	Are the data subjects unaware of the collection and processing of their information?		
3.	Does the activity involve the use of automated data collection from open sources?		
4.	Does the activity involve the use of new technology?		
5.	Does the activity include combining an individual's data from more than one source?		
6.	Is the personal information being used for a purpose different to what it was intended for?		
7.	Would the processing of personal data in this way be considered intrusive?		
8.	Will / might the data processing involve special categories of personal data? (please refer article 9 GDPR- Regulation (EU) 2016/6791[3])		
9.	Does the data processing involve decisions or assumptions being made about individuals?		
10.	Would the data subject consider the information being processed as private / sensitive?		

[3] Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Annex E Template 5 – Data Protection Impact Assessment

According to article 35 and 36 Regulation (EU) 2016/679 (GDPR) is for forms of processing, the "particular when using new technologies, due to the nature, scope, circumstances and the purpose of the processing are likely to pose a high risk to the Rights and freedoms of natural persons "have a priori Impact Assessment.

The assessment shall contain at least (please refer article 35 GDPR):

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 taking into account the rights and legitimate interests of data subjects and other persons concerned.

Risk assessments should be carried out from a strictly objective point of view. Reproduce the rows to include all actions that may raise data protection risks.

In principle, special categories of personal data are not collected in accordance with Art. 9 GDPR within the PROPHETS project. A Data Protection Impact Assessment is therefore not required.

RESEARCH OR DEVELOPMEMENT ACTIVITY			
1. Is the processing of personal data necessary to achieve the aims of the activity? 2. Has an alternative been considered? Please provide details: 3. Is the scale and type of the data processing proportionate to those aims? 4. Does the activity comply with data protection principles and requirements?			
Description of activity:			
Data Protection Officer or expert consulted for this exercise? Yes / No			
**Provide further information if ‘yes’ and justification or reasons if ‘no’:			
Actions Involving Data Protection Issues	Foreseeable Risks	Potential Consequences	
Mitigating Measure	Comments	Result	Evaluation

Annex F Template 6 – Records of Data Processing

In order to **demonstrate** compliance with data protection requirements, certain records should be kept. This will not only give a clear indication of the project's approach to such matters, but also will be crucial information in the case of a data breach.

PARTNER ORGANISATION:	
RESEARCHER / FACILITATOR:	
DESCRIPTION OF ACTIVITY:	
LEGAL FOUNDATION FOR ACTIVITY (See Article 6, GDPR)	
WHAT DATA WILL BE COLLECTED OR CREATED? (what type / volume/ format, any re-use of existing data?)	
HOW WILL THE DATA BE COLLECTED OR CREATED? (what procedures, how will data be organised?)	
WHAT ARE THE DATA SOURCES? (public, restricted, obtained directly or indirectly from the data subject?)	
HOW WILL THE DATA BE STORED AND BACKED UP? (organisational and technical security measures)	
HOW WILL YOU MANAGE ACCESS? (what are the risks? How will these be managed?)	
WILL THE DATA BE SHARED OR RE-USED? (any restrictions? Any risks? How will they be minimised? Data sharing agreement?)	
HOW WILL YOU MANAGE ETHICAL ISSUES? (any sensitive or confidential data? Written consent? Protect identity of participants?)	

References

[1] ALLEA (2017) 'The European Code of Conduct for Research Integrity, Revised Edition' [Online publication, All European Academies] **https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf**

[2] Council of Europe (1950) 'Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)' [Online publication, Council of Europe] **https://www.echr.coe.int/Documents/Convention_ENG.pdf**

[3] Council of Europe (2018) 'Convention 108 +' [Online publication, Council of Europe] **https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1**

[4] Council of Europe 'Data Protection Website' [Web pages, maintained, Council of Europe] **https://www.coe.int/en/web/data-protection/home**

[5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2009/977/JHA (Law Enforcement Directive) Available at: **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN**

[6] European Commission 'Data Protection in the EU' [Web page, maintained, European Commission] **https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en**

[7] European Commission (2018) 'Ethics and Data Protection' [Online publication, European Commission] **http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf**

[8] European Union Agency for Fundamental Rights (FRA) (2018) 'Handbook on European Data Protection Law' [Online publication FRA**]** **http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law**

[9] European Union (2000) 'Charter of Fundamental Rights of the European Union' *Official Journal of the European Communities*, C364/1 [Online publication, European Union] **http://www.europarl.europa.eu/charter/pdf/text_en.pdf**

[10] 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) Available at: **https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN**

[11] United Nations Office of the High Commissioner for Human Rights 'The Right to Privacy in the Digital Age' [Web page, United Nations, current and maintained] **https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx**

[12] United Nations (1948) 'Universal Declaration of Human Rights' [Web page, United Nations] **http://www.un.org/en/universal-declaration-human-rights/**