INDEED

Evidence – Based Model for Evaluation of Radicalisation Prevention and Mitigation

Deliverable No. 6.1

Gender, Ethical, Social and Legal Guidelines for the project's research activities and Gender, Legal, Social and Ethical Checklist for activity assessment

November 2021 (M3)

Authors: ***Norbert Leonhardmair (VICESSE), Hannah Reiter (VICESSE)***

Abstract:

This deliverable addresses the gender, ethical, legal and societal issues that may arise throughout the research activities of the INDEED project. Throughout the length of the project, activities will be monitored with regards to the presented guidelines.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Information table

Project Acronym	INDEED
Deliverable Number	6.1
Deliverable Title	Gender, Ethical, Social and Legal Guidelines for the project's research activities and Gender, Legal, Social and Ethical Checklist for activity assessment
Version	1.0
Status	Version Submitted to EC
Responsible Partner	VICESSE
Main authors	Norbert Leonhardmair (VICESSE), Hannah Reiter (VICESSE)
Contractual Date of Delivery	30.11.2021
Type	Report (R)
Actual Date of Delivery	30.11.2021
Dissemination Level	PU – public

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Document history

Version	Date	Status	Author	Description
0.1	8.11.2021	Draft	Norbert Leonhardmair (VICESSE); Hannah Reiter (VICESSE)	Initial draft
0.2	8-17.11.2021	Draft	WP Leaders (VUB, CENTRIC, UoH, KEMEA, PATRIR, VICESSE, DBL, PPHS)	Input to draft and review
0.3	17-26.11.2021	Draft	Norbert Leonhardmair (VICESSE); Hannah Reiter (VICESSE)	Integration of inputs
0.4	29.11.2021	Draft	Denitsa Kozhuharova (Ethical and Legal AB); Antonio Landi (Ethical and Legal AB)	Consultation with the INDEED Ethical and Legal Advisory Board Members
0.5	30.11.2021	PC and PMO accepted	Marzena Kordaczuk-Was (PPHS); Natalia Jarmuzek-Troczynska (PPHS)	Final review
1.0	30.11.2021	Submitted to EC	Marzena Kordaczuk-Was (PPHS); Natalia Jarmuzek-Troczynska (PPHS).	Final approval and submission

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Table of contents

List of tables

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

List of Acronyms

Acronym	Definition
INDEED	Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evidence-based model for evaluation of radicalisation prevention and mitigation
PVE	Prevention of Violent Radicalisation
CVE	Countering Violent Radicalisation
WP	Work Package
EBEM	Evidence-Based Evaluation Model
GELSA	Gender, Ethical, Legal, and Social aspects
GDPR	General Data Protection Regulation
TFEU	The Treaty on the Functioning of the European Union
SAB	Security Advisory Board
DMP	Data Management Plan
PSO	Project Security Officer
DPO	Data Protection Officer

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

1 INTRODUCTION

1.1 INDEED PROJECT OVERVIEW

INDEED aims to strengthen the knowledge, capabilities and skills of PVE/CVE and De-radicalisation first-line practitioners and policy makers in designing, planning, implementation and in evaluating initiatives in the field, based on evidence-based approach. INDEED builds from the state-of-the-art, utilising the scientific and practical strengths of recent activities – enhancing them with complementary features to drive advancements and curb a growing rise of radical views and violent behaviour threatening security.

The INDEED methodological framework is based on the '5I' approach i.e. 5 project phases: Identify; Involve; Innovate; Implement; Impact. At the core of INDEED's work methodology is an interdisciplinary and participatory approach, which includes the co-creation of individual project phases and implementing them with the close engagement of multi-sectoral stakeholders. The creation of SMART Hubs (Stakeholder Multisectoral Anti-Radicalisation Teams) as part of INDEED is intended to facilitate this process.

The selected results of the project are:

1. The Universal Evidence-Based Model (EBEM) for evaluation of radicalisation prevention and mitigation.
2. A practical EBEM-based Evaluation Tool.
3. A collection of user-friendly repositories (repositories of radicalisation factors and pathways into radicalisation; factors strengthening resilience to radicalisation. repositories of evidence-based practices) for practical use by practitioners and policy makers.
4. Targeted curricula and trainings (offline/online).
5. Lessons Learnt and Policy recommendations.

All results will be integrated and openly accessible in the INDEED multilingual Toolkit for practitioners and policy makers in the field for the entire lifecycle of PVE/CVE and De-radicalisation initiatives, from design to evaluation.

INDEED promotes the EU's values and principles; heeding multi-agency and cross-sectoral methods, including gender mainstreaming, societal dimensions and fundamental rights.

1.2 WP6 OVERVIEW

The main objectives of the Work Package 6 are:

1. Guarantee that the research is carried out complying with gender mainstreaming, fundamental rights, with the European Code of Conduct for Research Integrity and in line with applicable international, EU and national law and the GDPR.
2. Support practitioners and policy makers on increasing their awareness about gender, ethical, legal and social aspects on PVE / CVE / De-radicalisation initiatives.
3. Guide other WPs (WP2, WP3, WP5) in the production of content - reviewing their outcomes against the gender, ethical, legal and social implications of PVE /CVE/ De-radicalisation initiatives and their evaluation methods.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

4. Promote awareness of gender, ethical, legal and societal aspects among practitioners, policy makers and the general public.
5. Ensure that the INDEED's results will be gender, ethically, legally and socially acceptable and will not have a negative impact on those involved and targeted through its actions.

To achieve the following objectives, WP6 has four tasks and will deliver six deliverables, one of which is D6.1 Gender, Ethical, Social and Legal Guidelines for the project's research activities and Gender, Legal, Social and Ethical Checklist for activity assessment.

1.3 Executive Summary

This deliverable collects all the relevant principles (reliability, honesty, respect, accountability) in one comprehensive document to make sure that the research methodology will adhere to the European Code of Conduct for Research Integrity and that it will be in line with applicable international, EU, and national law. Since the contents of this deliverable are relevant to all the research activities of the project, it also takes into consideration data management (collection, storage, processing, retention and destruction of data), informing consent documents and procedures as well as information sheets which are aligned with all the General Data Protection Regulation (GDPR) policies.

In addition, this deliverable addresses the gender, ethical, legal and societal issues that may arise throughout the research activities of the project. Throughout the length of the project, activities will be monitored with regards to the presented guidelines. Monitoring will be performed with a gender, legal, data protection and ethical procedures checklist (see section 3) used by all partners while conducting the INDEED activities as well as delivering their results and outcomes. Special attention will be paid to the (non-biased) selection procedures of research participants; including informed consent procedures, the incidental findings policy and the mitigation strategy for the potential misuse of the research outputs.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Introduction

This deliverable prescribes the ethical standards and norms guiding the implementation of all INDEED activities implementing the project to be observed and upheld by all consortium partners. Going beyond that, D6.1 elaborates on the provisions of the proposal, detailing the standards, norms, procedures, practices and providing the corresponding supporting documents to be used by the consortium partners in implementing INDEED.

It is part of the overall INDEED approach to ethics, which encompasses the continuous ethical monitoring of the implementation of INDEED activities (T6.1), as well as the assessment of all INDEED outcomes and results (T6.4). In addition, it will assist other Work Packages to include the Gender, Ethical, Legal, and Social aspects (GELSA) with respect to PVE /CVE /De-Radicalisation practitioners' awareness (T6.2) and those of PVE /CVE / De-Radicalisation initiatives (T6.3).

INDEED's ethical approach has been integrated in the overall project design from the conception of the proposal. All project activities and tasks have been screened on the basis of the H2020 Guidance "How to complete your ethical self-assessment" and the emerging ethical issues addressed in Section 5 (in the Document of Action) and the prescribed requirements have then been acknowledged:

1. Human participation.
2. Personal data processing.
3. Incidental findings.
4. Misuse of research results.

In addition, D6.1 addresses the points raised by the European Commission's Ethics Summary Report in its Post-Grant Requirements. D6.1 has been co-developed with D9.1 to ensure that all information included is coherent, correct, and corresponding for the project consortium partners and the European Commission.

D6.1 has been reviewed by all WP leaders with respect to the correctness of the presentation of the individual tasks and activities. In addition, the external INDEED Ethical and Legal Advisory Board Members provided their feedback and opinion.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

2. ETHICS

INDEED seeks to comply with the tenants of Responsible Research and Innovation and with national and European research ethics requirements in a manner that is acceptable to stakeholders and society. The project is designed to involve practitioners and policy makers in the domain of PVE / CVE and De-radicalisation in order to create a universal Evidence-Based Evaluation Model (EBEM) for radicalisation prevention and mitigation which is verified against their needs and requirements and in tune with the core values of the European Union.

Some core ethical issues can emerge from INDEED project, therefore specific ethical safeguards are stated below in order to reduce and manage ethical risk and ensure ethical conduct throughout the research project.

2.1 HUMAN PARTICIPATION

The INDEED project follows a strongly participatory approach. Thus, it will involve human participants throughout its identify, involve, innovate, implement, and impact phase. There will be several activities involving human participants including forums, workshops, in-depth interviews, questionnaires, discussions, seminars/webinars, trainings, meetings, and annual events. Verification and validation methods will also involve human participants.

2.1.1 SELECTION PROCEDURE

INDEED will ensure a transparent and methodologically sound sampling strategy of interview participants, avoiding a discriminatory or biased approach to personally sensitive aspects, such as religion, political believes, gender, or ethnicity. Participants will be informed about the goal and implications of the research conducted including the use of their data.

Recruitment decisions will be made by the research organisation locally in consultation with other team members. The participants will be purposefully selected according to set criteria established prior to any data collection. INDEED will make sure that a wide variety of participants is selected specifically for the workshops, or any individual or group activity foreseen in the project (see table 1).

Recruits will be identified and selected according to scientific criteria on the basis of task-specific requirements. The criteria for target group identification can either be defined at the beginning of a task or can emerge in the course of the task after completing certain steps (e.g., identification of the field). In the respective method section of the task deliverables, the selection of the test subjects is specifically justified and explained.

2.1.2 INVITATION AND CONSENT

Participation in the research activities will be voluntary and no involvement of vulnerable groups or individuals is foreseen. Nevertheless, in order to gather data and better understand stakeholders' needs, the participation of practitioners will be needed. Participants will be healthy, adult volunteers who are in the position to understand and consent to our proposed research.

INDEED will procure informed consent from all volunteers participating in our study prior to the commencement of any data collection and participants will be informed that they can withdraw from the study at any time, without the need for explanation. No confidential personal

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

information will be retained. INDEED will demonstrate participants have understood these implications including their voluntary participations as well as anonymised processing of their data and any kind of use of this data. This will be outlined in a comprehensive informed consent procedure upheld by all research partners.

Participants will have the right:

- To know that participation is voluntary;
- To ask questions and receive understandable answers before making a decision;
- To know the degree of risk and burden involved in participation;
- To know who will benefit from participation;
- To know how their data will be collected, protected during the project and either destroyed or reused at the end of the research;
- To withdraw themselves and data from the project at any time;
- To know of any potential commercial exploitation of the research.

Copies of participant information sheets, the signed consent forms and confirmation of ethical approval from each institution is available to the European Commission (see attachments) and stored (for auditing purposes) by each partner (if applicable).

Written informed consent will be sought from all study participants. Participants are all mentally competent adults (i.e., aged 18+ years), able to give legal consent themselves.

Prospective participants will be provided with information about the study before any consent to participation is sought. They will be adequately informed about:

- The aim of the study and methods to be used;
- Institutional affiliations of the research and source of the funding;
- How participants will be selected and recruited, including inclusion and exclusion criteria;
- The setting in which they are asked to participate (survey, group discussion) and the duration and types of questions asked;
- Anticipated benefits;
- Potential risks and follow-up of the study; the description must demonstrate appropriate efforts to ensure fully informed understanding of the implications of participation;
- Discomfort it may entail;
- The right to abstain from participating in the study, or to withdraw from it at any time, without reprisal;
- Measures to ensure confidentiality of information provided, privacy and anonymity;
- Full contact details of the Data Protection Officer of the Coordinator in case questions may rise after the interview.

Standard consent forms have been developed for each type of participant and research technique.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Table 1: INDEED Types of Research activities/Data collection and Ethical Requirements

Task	Research activity	Description	Personal Data	Human Participants	Vulnerable Groups	Minors	Informed Consent Possible	Non-Eu Countries Involved	Large Scale Data Processing	Sensitive Data	Language	Requirements
T1.2	WP1 Research Forum	Research Forum with a group of academic experts and EU-funded project research staff will enrich the information gathered under WP1	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T2.1	Identification of key practitioner and policy makers stakeholders	The practitioners' engagement framework and a network of SMART Hubs that will form the basis of the multidisciplinary practitioner and policy makers engagement	Y	N	N	N	Y	N	N	N	N/A	Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

		throughout the project										
T2.2	Empirical data from practitioners and policy makers	Gap analysis carried out in this task will engage practitioners and policy makers	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T2.3	Practitioners Requirement Elicitation	MoSCoW method	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

											ensuring no lack of communication poses a risk.	Management Strategy
T2.2	WP2 Workshop	Co-creation workshop with SMART Hubs to develop solutions directly with practitioners, policy makers and relevant stakeholders	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T2.4	INDEED Baseline Report	In-depth analysis of the empirical work carried out in WP2	Y	N	N	N	N	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in	Data Protection and Management Strategy

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

										the language of participants ensuring no lack of communication poses a risk.	
T3.1 T3.2	Verifying the EBEM model and testing the EBEM-based Evaluation Tool	Verification of the EBEM model and testing of the EBEM-based Evaluation Tool by selected INDEED practitioners and policy makers, including SMART Hubs' stakeholders.	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	If applied: Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T4.1	Mapping and selection of PVE / CVE / De-radicalisation initiatives	Collection of initiatives for evaluation through the open call	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

	to be evaluated										partners native in the language of participants ensuring no lack of communication poses a risk.	inclusion/exclusion criteria); Data Protection and Management Strategy
T4.2	Conducting evaluation of PVE / CVE / De-radicalisation initiatives	Measuring the effectiveness and impact of initiatives against both qualitative and quantitative criteria, testimonials from the contact points of the evaluated initiatives.	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T4.3	WP4 Policy Recommendations Workshop	A 2-day workshop will be organised in order to enable an exchange of experiences and presentation of	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or	Informed consent procedures (Informed consent forms, Information sheets); Sampling

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

		outcomes derived from the 'Evidence-based evaluation and data analysis report'									by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T5.1	User-based identification of training/learning needs of practitioners and policy makers; Workshops at national level	In-depth interviews (in-person/via an online platform) and national level workshops to assess training and capacity building needs and requirements	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T5.2	Creation of innovative knowledge products	Video interviews, webinars, podcasts interviews	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationa	Informed consent procedures (Informed consent forms,

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

											lly in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T5.2	WP5 Forum "From Evidence to Practice; Towards Improved Policy&Practice"	Forum will bring together practitioners, practitioner agencies, leading experts, evaluators, policy makers and major EU agencies	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T5.5	WP5 Field trainings and Policy Seminar	In-person and online trainings; face-to face Policy Seminar, Trainers Community (including List of Trainers)	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

											consortium partners native in the language of participants ensuring no lack of communication poses a risk.	of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T6.2	Gender, Ethical, Legal and Social Aspects Practitioners' and Policy Makers' Awareness	Data on the existing level of awareness and identification of the needs and issues practitioners and policy makers may have on the domain of gender, ethical, legal, and societal aspects of PVE / CVE / De-radicalisation initiatives and their evaluation methods	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	Informed consent procedures (Informed consent forms, Information sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T6.4	Gender, Ethical, Legal and Social Acceptanc	A questionnaire ready-for-integration into the into the overall evaluation	Y	Y	N	N	Y	N	N	N	Activities will be conducted internationally in	Informed consent procedures (Informed consent forms, Information

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

	e and impact assessment	of the project results; online focus groups with practitioners, policy makers and civil society organisations									English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	sheets); Sampling strategy (Details of recruitment and inclusion/exclusion criteria); Data Protection and Management Strategy
T7.3	WP7 Project events	Project events organised to disseminate the INDEED's results	Y	Y	N	N	N	N	N	N	Activities will be conducted internationally in English or by local consortium partners native in the language of participants ensuring no lack of communication poses a risk.	Data Protection and Management Strategy

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

2.2 Data Protection

The INDEED project acknowledges that data protection is a fundamental right, implemented within the Treaties of the European Union: The Treaty on the Functioning of the European Union (TFEU) and the Charter of Fundamental Rights. The European law setting out the new protection of individuals' rights and increasing data controller obligations in the digital era is the General Data Protection Regulation (GDPR). This is the main law that will apply to the project's research and development activities. The project involves the collection and processing of personal data; to correctly implement this within INDEED the following definitions will be included within the project's taxonomy as defined in GDPR:

- Personal data: "[…] any information relating to an identified or identifiable natural person ('data subject'); and 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 physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.";
- Data Processing: "[...] any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.";
- Data Controller: "[...] 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: "[...] a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; […]."

The GDPR establishes a risk-based approach to data processing and requires data controllers to bear full responsibility for the safety and security of personal data and the protection of individuals' rights in relation to the processing of their personal data. The INDEED project will fully endorse and adopt this approach, mirroring it in the research processes and practices throughout and beyond the project. In particular, INDEED will strictly adhere to the GDPR Framework, which highlights the key principles for collecting and processing data:

- Lawfulness: INDEED will only process data for a specific purpose and remain transparent with the users;
- Purpose limitations: INDEED will collect and process data for specified and legitimate purposes, following explicit consent from the users;
- Data minimisation: INDEED will limit the amount of data collected and retained where necessary;
- Data accuracy: INDEED will ensure the data stored is accurate, up to date and secured safely;

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

- Storage limitations: The data will be kept for as short-term as possible, and where applicable pseudonyms[1] will be used to protect user identities;
- Integrity: The data processors of the research will protect user data against unlawful processing or loss, using encryption and privacy by design methods.

2.2.1 DATA COLLECTION AND PROCESSING

The INDEED research does involve personal data collection and processing, however personal data will not be of sensitive nature. INDEED will design and uphold a rigorous data protection strategy and management, having devoted T8.1 Data Management Plan (D8.2) to it, ensuring the anonymity of the participants by removing all direct or strong indirect personal identifiers. The Data Protection Plan will be documented and enforced by all research partners in the consortium.

Only relevant (personal) data will be collected and no more than what is needed for the research study. In general, quotes will be de-identified. However, data included in the study (e.g., quotes, materials, survey responses from gatekeepers, etc.) can potentially be traced back to identifiable persons. If identifiability occurs, the data associated will be excluded from the research.

Furthermore, the research team will adopt methods and procedural measures in relation to matters such as data recording style, personal identifiers, transcription and processing procedures, lifespan of unprocessed data, type and places of storage, and put all measures in place for data safety. Specifically, all data will be kept separately from identifying information. The researchers will store relevant information securely and the INDEED consortium will set protocols in the Data Management Plan, for how such data will be accessible by others and its access at a local level.

[1] A detailed description of anonymisation and pseudonymisation procedures will be featured in D9.3 (M6) as foreseen in the Post-Grant Requirements of the European Commission.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

In accordance with GDPR art. 7.3 participants can withdraw their data whenever they wish, but the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. If possible, participants are offered the opportunity to correct factual errors and withdraw certain quotes (of their own – not of others in case of focus groups).

2.2.2 DATA PROCESSING & STORAGE DURING THE PROJECT

During the research, data will be stored securely in locked file cabinets; an end-to-date end-encrypted secure environment. The Data Management Plan will contain information on which data need to be stored for how long and which data need to be destroyed. Researchers receive adequate support and supervision from the Coordinator.
All envisaged data collection activities and the planned data management strategy across the whole Data Life Cycle are listed in table 2.

Contact data of research participants will be collected guided by a strategy ensuring a non-discriminatory sampling. They feature the name, organisation (if applicable), and contact details of the research participant. Contact data of participants will be stored in password protected files by the partner organisation conducting the research and will not be used for further analysis and omitted from datasets for analysis. Contact data will not be shared within the consortium or with external partners/third parties and will be deleted after the research activities have been finalised.

Informed consent forms will be collected by partner organisations conducting the research. They feature the name, organisation, contact details, and signature of the research participant. Informed consent forms will be stored as non-digital hard copy in a locked file cabinet by the partner organisation conducting the research. These forms will not be used for further analysis or shared with external partners/third parties and omitted from datasets for analysis. Informed consent forms may be available to the Coordinator upon prior inquiry and sent in a secure way.

All consent forms will be located with each respective partner and stored in a secure locked file cabinet; all hard copies will be destroyed five years after project completion.

Research partners who conduct the field study collect audio recordings of the interviews/focus groups. The audio files will remain at the partner organisation conducting the research. The audio files will be password protected. The recording devices will be stored in a locked file cabinet. Audio recordings will be transcribed as protocols, any identifiable information (direct or strong indirect identifiers) will be omitted from the transcripts. Analysis will be done by partner organisations conducting the research without any involvement of third parties. Audio recordings will remain solely at the national research partner organisation and not shared with the consortium or third parties. The recordings will be deleted after they have been transcribed into protocols.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Transcripts/Protocols of interviews/focus groups will be created on the basis of audio recordings. Any identifiable information (direct or strong indirect personal identifiers) contained within the interviews will be omitted from transcripts, including personal/contact data. Transcriptions/Protocols will be stored as document files digitally at the respective partner organisation. While they do no longer include personally identifiable data, partner organisations will store them in password protected files. Transcriptions will be analysed by those partner organisations who collected the data, or consortium members with expertise in qualitative research methods. Findings omitting identifiable information and translated excerpts/protocols will be shared within the consortium. Appropriate security measures (file encryption) will be taken. The data won't be stored in unprotected cloud services, shared with third parties, or made publicly available. Transcriptions/Protocols will be stored in digital files by the partner organisations who collected them for five years after the project concludes; all copies will be destroyed by consortium members afterwards.

The consortium members will sign a Data processing agreement according to § 28 GDPR encompassing the types of data, involved tasks, types of (secondary) use, as well as delineating data controllers and processors and the requirements and use conditions (see Annex 5.3). The DSA will be signed before any research activity involving personal data collection starts and submitted to the European Commission as part of D9.3 (Requirement No. 3; Description of the anonymisation/pseudonymisation techniques that will be implemented) .

2.2.3 Risk Management

The consortium is aware of the applicable laws and regulations. All risks are assessed in consultation with the owner. Data are considered classified and handled accordingly. Privacy risks are assessed on the basis of the Data Management Plan (DMP). If new major risks are identified these shall be recorded. The Initial Risk Management Plan (Deliverable 8.3) refers to potential general as well as task-specific risks of the project and addresses these accordingly. Further, risks are mitigated in the Data processing agreement (Annex 5.3).

2.2.4 Further Processing of Previously Collected Data

INDEED will further process data which has been previously collected for academic purposes for secondary analysis complying with any provision of the GDPR or national data protection laws. Existing data sets will be listed in the Data Management Plan and checked to not include personally identifiable data, as well as to their accuracy and their lawful establishment. For any further processing of previously collected data partners will demonstrate their legal basis for data processing as well as the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects. This will be detailed in D9.3 as foreseen in the Post-Grant Requirements of the European Commission.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Table 2: Data types and Data management strategy across the Data Life Cycle

Data type	Personal data	Public data	Anonymised data	Collection	Storage	Analysis	Sharing	Deletion
Contact data of participants	yes	no	no	Contact data of research participants will be collected guided by a strategy ensuring a non-discriminatory sampling. They feature the name, organisation (if applicable), and contact details of the research participant.	Contact data will be stored in password protected files by the partner organisation conducting the research.	Contact data will not be used for further analysis and omitted from datasets for analysis.	Contact data will not be shared within the consortium or with external partners/third parties.	Contact data will be deleted after the research activities have been finalised.
Informed consent forms	yes	no	no	Informed consent forms will be collected by partner organisations conducting the research. They feature the name, organisation, contact details, and signature of the research participant.	Informed consent forms will be stored as non-digital hard copy in a locked file cabinet by the partner organisation conducting the research.	Informed consent forms will not be used for further analysis and omitted from datasets for analysis.	Informed consent forms will not be shared with external partners/third parties. Informed consent forms may be available to the coordinator upon prior inquiry and sent in a secure way.	All consent forms will be located with each partner and stored in a secure locked file cabinet; all hard copies will be destroyed five years after project completion.
Audio recordings of interviews/focus groups	yes	no	no	Research partners who conduct the field study collect audio recordings of the	The audio files will remain at the partner organisation conducting the research. The audio	Audio recordings will be transcribed as protocols, any identifiable information (direct or strong indirect	Audio recordings will remain solely at the national research partner organisation and not shared with the	Audio recordings will be deleted after they have been transcribed into protocols.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

				interviews/focus groups.	files will be password protected. The recording devices will be stored in a locked file cabinet.	identifiers) will be omitted form transcripts. Analysis will be done by partner organisations conducting the research without involvement of third parties.	consortium or third parties.	
Transcripts/ Protocols of interviews/ workshops	yes	no	yes	Transcripts/Protocols of interviews/focus groups will be created on the basis of audio recordings. Any identifiable information (direct or strong indirect personal identifiers) contained within the interviews will be omitted from transcripts, including personal/contact data.	Transcriptions/Protocols will be stored as document files digitally at the partner organisation. While they do no longer include personally identifiable data (and only anonymised data), partner organisations will store them in password protected files.	Transcriptions will be analysed by partner organisations who collected the data, or consortium members with expertise in qualitative research methods.	Findings omitting identifiable information and translated excerpts/protocols will be shared within the consortium. Appropriate security measures (file encryption) will be taken. They won't be stored in unprotected cloud services, shared with third parties, or made publicly available.	Transcriptions/Protocols will be stored in digital files by the partner organisations, who collected them, for five years after the project concludes and all copies destroyed by consortium members afterwards.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

2.3 Incidental Findings Policy

Addressing the possibility of discovering incidental findings and describe in advance the procedure that shall be followed in such case acting both proactively (for instance acquiring consent forms by the participants), as well as following such findings (confidentiality, communication to research participants etc.) is an ethical requirement in all research that involves human participants.

If this is the case, namely a human subject research, the procedures that will be implemented in the event of unexpected incidental findings should be clearly stated (namely whether the participants have the right to know or not to know about such findings or statements of participants can trigger actions with consequences to them). Researchers have an obligation to address the possibility of discovering incidental findings and describing in advance the procedure that shall be followed in such case.

If one considers the ethical implications such findings may raise for researches and at the same time what implications their disclosure to participants may present, it becomes apparent that incidental findings present a range of ethical, legal, and practical challenges, for both their recipients, as well as the researchers who encounter them.

The notion of incidental findings originated in medical and genetic research. An anticipatable incidental finding is one that is known to be associated with a test or procedure. Anticipatable incidental findings need not be common or even likely to occur—their defining characteristic is that the possibility of finding them is known. Anticipatable incidental findings include findings that could not have been anticipated given the current state of scientific knowledge. Researchers cannot plan for these types of findings specifically. However, they can consider in advance what they might do if a particular kind of unexpected finding arises, for example, one that could be actionable or lifesaving.

As far as researchers are concerned the main ethical concern that needs to be addressed is: are researchers ethically obligated to share such information with study participants and, if yes, are they qualified to do so? This obligation derives from the broader researcher duty of beneficence to secure participants' well-being by maximizing benefits and minimizing harms. In other words, researchers have an ethical duty to plan for incidental findings to the best possible extent.[2]

INDEED's general policy is that any researcher who is involved in activities involving human participation and data processing discovers incidental findings (of unspecified nature) shall inform the WP leader, the Project Security Officer, the Data Protection Officer, and Coordinator of INDEED. This shall remove the burden of an individual researcher to decide the course of action. This group will decide upon the evidence of the incidental finding, carry out, if necessary, a risk assessment procedure, consult with external / or national advisors, if necessary, to establish the necessary legal framework or other relevant context facts, while protecting the privacy of the research participant. And shall then decide whether to inform the research participant; not inform the research participant; involve any other authority relevant to the incidental finding. Meeting minutes and decisions should be documented in writing and kept confidential by the Coordinator.

2 https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c7c9a499&appId=PPGMS; https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2581517/

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

2.4 Misuse of Research Results

The INDEED consortium partners share an awareness of the specific risks of misuse related to research findings and have experience in the application of successful counter measures. The Coordinator will implement a special internal review process screening deliverables and materials to be made publicly available with regard to their potential misuse. Adequate wording and explanatory notes will be added in all those cases where a risk of strategic misuse is identified. It is worth mentioning, that INDEED's project management structure includes a Security Advisory Board (SAB). The SAB consists of independent experts who will provide advice to the INDEED project concerning security issues. They will assess the sensitivity and potential of misuse of deliverables prior to publication. The SAB will ensure the compliance of all security rules and re-assess the sensitivity of each deliverable as well as the level of dissemination of each prior to publication.

The consortium has already been sensitised to the issues of misuse of data/findings/dissemination by previous research in sensitive areas. In addition, many partners have carried out work in the area of documenting, analysing and preventing racism, xenophobia, hate crime, misogyny and homophobia. The project has appointed Mr Babak Akhgar from CENTRIC Sheffield Hallam University as Project Security Officer (PSO) within the Grant procedure who will provide the latest advice and recommendations of concerns within a security context. The PSO will heed advice and guidance provided by the advisory boards but is the responsible actor for reviewing the deliverables regarding their potential sensitive nature, misuse, and determining whether adjustments are required.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

3. SOCIETAL IMPACT

The INDEED consortium understands social impact as the effect that all project activities and results will have on people (individuals) and entire communities. All planned medium- and long-term impacts will be achieved through the use of evidence-based approaches to strengthen first-line practitioners' and policy makers' knowledge, capabilities and skills for the designing and evaluation of PVE/ CVE / and De-radicalisation initiatives (such as policies and strategies, programmes, actions and interventions). Below is an explanation on how INDEED will impact society by caring for the gender, ethical and social aspects relating to particularly sensitive areas of social life in the context of PVE / CVE and De-radicalisation initiatives.

3.1 SOCIETAL SECURITY NEEDS

The guiding principle of the INDEED project is to treat societal security, related to all dimensions such as life, liberty, health, employment, property, environment as well as values, as a key factor ensuring the high quality of life of EU citizens by preventing and countering current threats. Therefore, INDEED intends to produce outcomes that will provide policy makers and practitioners with the necessary skills and knowledge in order to design, plan, implement, and evaluate future activities meeting the scope and objectives of the EU Internal Security Strategy, thus reinforcing the realisation of a comprehensive European Security Model. Starting from the research conducted in WP1, to the development of final practical solutions (WP3, WP5), particular attention will be paid to the search for well-established scientific approaches to the evaluation of practical initiatives corresponding to the real social needs in the field of security, i.e., responding to the diagnosed real causes and paths leading to radicalisation and addressed to the general public society. Additionally, particular attention will be paid to initiatives addressed to groups that are particularly vulnerable or at risk of radicalisation.

The INDEED research output from WP1 and WP2 is going to meet societal security needs in two ways: Through developing a universal Evidence-Based Evaluation Model for radicalisation prevention and mitigation along with an interactive evaluation tool, tailored to the different types of policy makers and first-line practitioners, which will be easily adjustable to their specific needs and requirements from the field as well as to the specific needs of local communities they operate in. This will be possible via developing a multidisciplinary, multi-agency, and multi-stakeholder approach based on real, face-to-face, user-oriented interaction and exchange between academics and practitioners. The specific results of the project will be tested and validated in SMART Hubs and other workshops and will be evaluated based on the KPI's that the Consortium has set (WP3, WP4, WP5). The gender, ethical, legal, and societal acceptance of the INDEED tools and other results will proceed in WP6 by conducting a robust impact assessment and validating the outcomes by civil society organisations as well as directly by citizens. The project will carry out a survey to assess the acceptance of results. As a next step 5 online focus groups with the participation of practitioners and civil society organisations will take place to collect opinions on the already formed questionnaires. The experts invited to the Ethical and Legal Advisory Board will be strongly involved in the ethical, legal and social acceptance assessment. The requirements and findings will be disseminated and discussed to a wide stakeholder group, and this will open for discussion and reflection on how well societal needs are met.

3.2 THREATS TO SOCIETY

INDEED responds to the need for ethically enhanced knowledge, capabilities, and skills of policy makers and first-line practitioners in the area of PVE / CVE / De-radicalisation, accepting the premise that radicalisation leading to violent extremism is a contemporary global threat, posing

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

many additional challenges not only for law-enforcement agencies, but also for the general public. Specifically, the project aims at providing a universal Evidence-Based Evaluation Model for radicalisation prevention and mitigation together with an interactive EBEM-based Evaluation Tool dedicated to PVE / CVE and De-radicalisation initiatives. This universality will be based, inter alia, on the applicability of these results to various forms of radicalisation leading to violent extremism (from jihadi terrorism, through left- and right-wing extremism), but also in line with the current trends and changes in radicalisation processes related to COVID-19, anti-5G movements, increasing threats of individual radicalisation or increased importance of online channels in recruiting. In addition, they will be applicable to initiatives designed and implemented in other areas of security threats' prevention and crime prevention. INDEED also includes real time, dynamic capacity building activities, along with training packages, and a toolkit to support policy makers and first line practitioners, improving their resilience and consequently securing the public (potential victims) from PVE, CVE and crime related threats.

Addressing threats in an appropriate way means that the INDEED consortium fulfils the highest standards of research integrity and H2020 ethics requirements, considering also the national legal frameworks for PVE/ CVE / De-radicalisation and other, crime related threats' prevention and mitigation and the protection of the fundamental rights and freedoms of individuals. Importantly, this correct addressing of threats by the INDEED consortium also includes the issue of gender awareness and gender mainstreaming, which is treated as a general principle and as a cross-cutting priority that guides all designed project activities. Therefore, INDEED devotes a full work package (WP6 objectives and tasks) to ensuring these standards. The consortium's composition and the expertise of the staff engaged in the project are a decisive factor for its successful implementation.

3.3 Societal Benefit

INDEED is dedicated to providing first-line practitioners policy makers enhanced competencies on efficient evidence-based designing, planning, implementation and evaluation of PVE / CVE / De-radicalisation as well as prevention and mitigation of other crime related threats. It also aims at facilitating the smooth cooperation among specific groups of policy makers and first-line practitioners representing LEA, local authorities, prison and probation, social and health services, education, civil society organisations, and other relevant actors in the field of PVE / CVE and De-radicalisation (WP2, WP5). Selected risk factors/pathways into radicalisation and specific risk groups constitute the main criteria in the selection of initiatives (polices and strategies, programmes, actions and interventions) that will be analysed in terms of approaches used for their evaluation (WP4). At this stage, the analysis focuses on both scientific sources and practical solutions (initiatives) addressed primarily to groups vulnerable or at risk of radicalisation such as: children and young people, returnees, with a focus on children and women; extremists after their release from prison; as well as lone actors.

While special attention is paid to those social groups mentioned above, which are particularly at risk of radicalisation leading to violent extremism, society as a whole will benefit from the increased security as a result of enhanced capabilities and efficiency in designing, planning, implementation and evaluation of initiatives dedicated to the PVE / CVE / De-radicalisation, and other threats' prevention and mitigation. The sources analysed in WP1 and WP2 will concern initiatives that take into account all current trends in radicalisation, and thus respond to the real security needs of all social groups. Moreover, the EBEM model and EBEM-based Evaluation Tool developed in WP3 will be universal, which means that they will be applied to initiatives planned at all levels of prevention and mitigation (primary, secondary and tertiary) and addressed to various audiences, i.e., all individuals at risk or affected by radicalisation. Moreover, this universality also means suitability for use by all first-line practitioners and policy makers, no

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

matter what sector or agency operating in the field of PVE / CVE or De-radicalisation they represent.

3.4 European Societal Values

Human dignity, strengthened community involvement, and sustainable development will be enhanced thanks to INDEED research outcomes, evidence-based practical results, and tailor-made trainings related to the increasing effectiveness of initiatives dedicated to PVE / CVE and De-radicalisation. According to the assumptions of effective prevention of security threats, which is part of the paradigm of social as well as crime prevention, INDEED focuses on the individuals and their individual needs, as well as on the impacts based on a community- and family-based approach. Initiatives based on these approaches are not only particularly effective, but also allow to focus on the human aspects when dealing with PVE/ CVE/ De-radicalisation and crime related threats' prevention and mitigation.

3.5 Research Impact

The research will not have any negative impact neither on society nor on the rights and values enshrined in the Treaties (e.g. freedom of association, freedom of expression, protection of personal dignity, privacy and data protection). This task is dedicated to the early detection of any issues regarding privacy and data protection and to the mapping of proper legal and ethical requirements in accordance with international, EU and national legislation and ethical principles, which can serve as a guide during the project's implementation. In addition, T6.4 is devoted to analysing the Gender, Ethical, Legal and Societal Impact of INDEED results, preserving the project on track with the high EU standards.

The research could not impact disproportionately upon specific groups or unduly discriminate against them. The internal ethics and legal team along with the external Ethical and Legal Advisory Board will ensure that if such issues were to arise, they will be handled promptly, pertinently, and with due respect for fundamental rights and values.

The INDEED project is compliant with the mandates of the Charter of Fundamental Rights of the European Union, as well as the European Convention on Human Rights of the Council of Europe. The project is directly affecting citizen safety by providing an optimised way to assist first-line practitioners' and policy makers' efforts in the area of PVE / CVE and De-radicalisation. Both, the results of the research (WP1, WP2, WP4) as well as all practical results (WP3, WP5) are taking thoroughly into consideration the universal values of human dignity, life, health, freedom, liberty, respect for private life, personal data protection and property.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

4. INTEGRATED INDEED ETHICS CHECKLIST

4.1 HUMAN PARTICIPATION CHECKLIST

- I have made sure that no vulnerable groups or individuals have been selected for the planned research;
- I have made sure that the selection of participants is comprehensible and non-discriminatory/non-biased;
- I have made sure participation in the research is voluntary;
- Participants have been adequately informed about the study, their involvement and any relevant ethical implications (e.g. use of data);
- Participants have read, understood, and signed the informed consent forms used throughout the INDEED project.

4.2 DATA PROCESSING CHECKLIST

- I have made sure the anonymity of research participants is ensured by removing all direct or strong indirect personal identifiers;
- I have made sure that all data is kept separately from identifying information;
- I have made sure that all data is stored safely (in locked file cabinets) and only shared with relevant partners;
- I have checked existing data sets (previous research) to not include personally identifiable data as well as to their accuracy and their lawful establishment.

4.3 INCIDENTAL FINDINGS CHECKLIST

- I have encountered an incidental finding during research involving human participants or resulting data processing;
- I have documented the incidental finding and informed the WP leader, the Project Security Officer, the Data Protection Officer, and the Coordinator (team) in a timely manner;
- The team have reached a decision whether to inform the participant, not to inform the participant, inform any other authority/body, and whether to include the finding in the research results.

4.4 MISUSE OF RESEARCH RESULTS CHECKLIST

- Prior to the publication of a deliverable, I have checked with the Project Security Officer (PSO) and the Security Advisory Board (SAB) concerning any potential misuse of the deliverable;
- I have made sure that the research findings do not impact disproportionately upon specific groups or unduly discriminate against them;
- I have made sure that the research does not have any negative impact neither on society nor on the rights and values enshrined in the Treaties (e.g. freedom of association, freedom of expression, protection of personal dignity, privacy and data protection).

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

5. ATTACHMENTS

5.1 INFORMED CONSENT FORM

Project Acronym: INDEED
Project Title: Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evidence-based model for evaluation of radicalisation prevention and mitigation
Grant Agreement No: 101021701

INDEED Informed Consent Form

I _____ [name of participant] agree to participate in this INDEED [interview / focus group / training / workshop].

The purpose of the [interview / focus group / training / workshop] has been explained to me in writing (in the information sheet).

I am participating voluntarily and understand that I can withdraw from the [interview / focus group / training / workshop] without repercussions, at any time, by contacting the Data Protection Officer either by sending an e-mail to norbert.leonhardmair@vicesse.eu [e-mail address of the DPO] or by calling +4319296645 [telephone number of the DPO].

I have been fully informed how the protection of my data will be ensured and I am satisfied that the assurances of responsible and strict data governance, given by the INDEED project, will be upheld.

I understand that anonymity, by removing any identifying information from protocols and transcripts will be ensured at each research stage in the project.

A copy of the information sheet and (this) signed consent form has been given to me (the signee).

- ○ I consent to participate in this [interview / focus group / training / workshop].
- ○ I consent to the processing of my personal data.

[Signature participant]

[City], [Date]

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

5.2 Invitation Letter & Project Information Sheet

Project Acronym: INDEED
Project Title: Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evidence-based model for evaluation of radicalisation prevention and mitigation
Grant Agreement No: 101021701

Invitation to participate in an INDEED [interview / focus group / workshop]

Dear [first name] [last name],

I am writing to you on behalf of the **INDEED project** (Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evidence-based model for evaluation of radicalisation prevention and mitigation). It is a 36-months EU-funded project aiming to strengthen the knowledge, capabilities and skills of **PVE/CVE and De-radicalisation** first-line practitioners and policy makers in designing, planning, implementing, and evaluating initiatives in the field, based on an evidence-based approach. As part of INDEED's research, a [interview / focus group / workshop] will be done, designed to collect information on **current practices of de-radicalisation strategies, programmes, and their evaluation**.

INDEED is a research and innovation project that builds from the state-of-the-art, utilising the scientific and practical strengths of recent activities – enhancing them with complementary features to drive advancements and curb a growing rise of radical views and violent behaviour threatening security. INDEED is designed to provide evidence-based and practical solutions ready for use by a variety of policy makers and first-line practitioners (representing LEAs, local authorities, prison and probation, social and health services, education, civil society organisations), and other relevant actors in the field of PVE / CVE and De-radicalisation. INDEED will develop a practical and interactive **Toolkit** for PVE/CVE and De-radicalisation first-line practitioners and policy makers. This will enable and support the rapid response of its end-users to unexpected risk factors that appear in a specific period of time (such as, for example, reactions to the threat of radicalisation during the COVID-19 pandemic, or those caused by the movement against 5G technology).

I am asking for **your participation** in a(n) [interviews / focus groups / workshops] that will run from [date] to [date] in [location].
This research is carried out as part of [Task title] with the aim [short task description].

The INDEED project team assures that any personal data or information you provide will be kept strictly **confidential** and will be securely stored and kept for the lifetime of the project and deleted 5 years after the project's conclusion.

Furthermore, should you agree to participate, and subsequently feel unable or unwilling to continue, you are free to leave without negative consequences. Your participation is completely voluntary, and you may withdraw from this project at any time.

An **information sheet**, which describes the project in more depth, has been prepared (see attached) to aid in making a fully informed decision on participation.
Should you agree to participate, after understanding and accepting the requirements of participation, we will provide you with a **consent form** on the day of the [interviews / focus groups / workshops] that will formalize the conditions of your participation.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Should you require further information about the project, I please don´t hesitate to contact me for further information. Alternatively, should you not be in a position to participate, we would appreciate any assistance in finding a suitable replacement.

Looking forward to your response.

Sincerely,

[Title] [First name] [Last name]
[Position], [Partner organization name]

Attachment: INDEED Project information

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Project Acronym: INDEED
Project Title: Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evidence-based model for evaluation of radicalisation prevention and mitigation
Grant Agreement No: 101021701

INDEED Information sheet

INDEED is a 36-month EU-funded project aiming to strengthen the knowledge, capabilities and skills of PVE/CVE and De-radicalisation first-line practitioners and policy makers in designing, planning, implementation and in evaluating initiatives in the field, based on evidence-based approach. The INDEED project requires that professionals who participate in the [interviews / focus groups / workshops] give explicit consent to do so.

Please take time to read and understand the following information and if you agree with the content sign the consent form.

I freely and voluntarily consent to be a [interviews / focus groups / workshops] participant in the INDEED project to be conducted by [partner] on [date] at [location]. The person(s) responsible for collecting the data is/are _____ [name of data processor] of the organisation _____ [organisation name] and can be reached by me at any time at _____ [mail address].

The INDEED project team ensures that any data or information you provide will be kept strictly confidential. In gathering our data, we will only record information that is necessary to address the central purpose of our research and ensure that your information given will be anonymized. Information will be securely stored and retained for the lifetime of the project and deleted 5 years after the project's conclusion. The legal basis for the processing of the data is consent, as provided by the INDEED project consent form.

Your name will not be linked with the research materials, as the researchers are interested in the content in general, and not in any individual's opinions or choices. Results from the interviews can be included in project deliverables, communication material (primary use) and academic publications (secondary use). However, any directly or indirectly identifiable data will be omitted to guarantee the anonymity of the interviewee.

A general commitment of the researcher applies to treat the information provided by the research participants pseudonymously, i.e., not directly linkable to him/her, and without repercussions for what they disclose to the researcher. Unlawful behaviour reported by the interviewee will be reported to the Coordinator. Such "incidental findings" will be dealt with according to the Criminal Law procedures of the INDEED member countries.

I understand that if at any time during the pilot test I feel unable or unwilling to continue, I am free to leave without negative consequences. That is, my participation in this [interview / focus group / workshop] is completely voluntary, and I may withdraw from this project at any time. I further have the right to request the following from the data controller: access to and rectification or erasure of my personal data, restriction of processing concerning the data subject, object to the processing of data, right to data portability. You further have the right to withdraw your consent at any time or lodge a complaint with a supervisory authority.

Potential risks of participating in this research may be the risk of entrusting your personal data in the hands of others, and the potential harm for misuse of those identifiable data. The

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

reassurances around strict data governance, given by the INDEED team, are designed to alleviate potential participation burdens.

On the other hand, the benefits of participating in this research are twofold: it provides you with a rare opportunity to be involved in a significant piece of research; the role you play in improving the evaluation of PVE/CVE and De-radicalisation practices will provide you with great self-satisfaction in the future.

I have been informed that if I have any questions needing further clarification or assurances about the ethical issues relating to the project, I am free to contact Norbert Leonhardmair, Norbert.leonhardmair@vicesse.eu, VICESSE or Hannah Reiter, Hannah.reiter@vicesse.eu, VICESSE.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Project reference details - Overview

Call: H2020-SU-SEC-2018-2019-2020 (Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism)
Topic: SU-FCT01-2018-2019-2020
Type of action: Research and Innovation Action (RIA)
Project Acronym: INDEED
Project Title: Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evidence-based model for evaluation of radicalisation prevention and mitigation
Grant Agreement No: 101021701
Project website: www.indeedproject.eu
National partner contact: [Partner contact first name/last name], [Partner e-mail address], [Partner organization name]
Coordinator contact: Marzena Kordaczuk-Was: contact@indeedproject.eu, PPHS
Project Manager and Project Management Office: office@indeedproject.eu; natalia.jarmuzek@ppbw.pl, PPHS
Data Protection Contact: Norbert Leonhardmair, Norbert.leonhardmair@vicesse.eu, VICESSE

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

5.3 DATA PROCESSING AGREEMENT

Project Acronym: INDEED
Project Title: Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evidence-based model for evaluation of radicalisation prevention and mitigation
Grant Agreement No: 101021701

Data Processing Agreement — INDEED

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between

_____
_____
_____
(the "Company") and

_____
_____
_____
(the "Data Processor")
(together as the "Parties")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with 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).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

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

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "Contracted Processor" means a Subprocessor;

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

1.1.5 "EEA" means the European Economic Area;

1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.8 "Data Transfer" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "Services" means the _____ services the Company provides.

1.1.10 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel
Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within

10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of _____.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of _____, subject to possible appeal to _____.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Your Company
Signature _____
Name: _____
Title: _____
Date Signed: _____
Processor Company
Signature _____
Name _____

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701

Title _____
Date Signed _____

This project has received funding by the European Union's Horizon 2020 research and innovation programme H2020-SU-SEC-2020 under grant agreement no 101021701