DYNAMO

D1.3

Ethical and Legal Protocol and Compliance Assessment

Project number	101069601
Project acronym	DYNAMO
Project title	Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors
Start date of the project	1st October, 2022
Duration	36 months
Programme	HORIZON-CL3-2021-CS-01

Deliverable type	Report
Deliverable reference number	SC1-DTH-07-101069601/ D1.3 / 1.0
Work package contributing to the deliverable	WP1
Due date	March 2024 – M18
Actual submission date	27th March 2024

Responsible organisation	KEMEA
Editor	Georgia Melenikou
Dissemination level	PU
Revision	V1.0

Abstract	Task 1.4 aims to identify the ethical and legal aspects of the DYNAMO project and to assess compliance of (a) the research and (b) the project's technological solution with the current ethical and legal framework. D1.3 constitutes the official report.
Keywords	Research, ethics, gender, legal framework, requirements, compliance

The project DYNAMO has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101069601.

Editor

Georgia Melenikou (KEMEA)

Contributors (ordered according to beneficiary numbers)

All partners

Document control			
Version	**Date**	**Author(s)**	**Change(s)**
0.1	05.05.2023	Georgia Melenikou (KEMEA)	Skeleton
0.2	29.05.2023	Georgia Melenikou (KEMEA)	Ethics guidelines & collection of input
0.3	31.10.2023	Georgia Melenikou (KEMEA)	Chapter on research ethics & organisation of the collected input
0.4	12.12.2023	Georgia Melenikou (KEMEA)	Chapter on legal framework and requirements
0.5	23.01.2024	Georgia Melenikou (KEMEA)	Addition of input & finalisation of chapters
0.6	09.02.2024	Georgia Melenikou (KEMEA)	Ready to send for Consortium and peer review
0.7	14.03.2024	Dalila Antunes (FS)	Peer review
0.8	17.03.2024	Dr. Karen Neville (UCC)	Peer review
0.9	22.03.2024	Georgia Melenikou (KEMEA)	Incorporation of peer reviewers' comments and updates due to the legislative developments (AI Act)
1.0	27.03.2024		Ready to submit

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

This document is drafted as part of T1.4 ‘Ethical & Legal Aspects and Compliance Assessment’ and constitutes the official report of that task which aims to present the identified ethical and legal issues relating to the DYNAMO project and to assess compliance of (a) the DYNAMO research and (b) the DYNAMO technological solution with the existing ethical and legal framework.

According to the description in the Grant Agreement, “D1.3 reports the legal / ethical framework that must be respected in the development of the DYNAMO solution and includes an assessment on the compliance of the solution to it. It will also include an updated version of the internal guide of M07”.

The deliverable is divided in two main parts. The first part is focused on the research activities, the potential ethical and legal risks and the appropriate mitigating actions that need to be taken by the DYNAMO Consortium during the lifetime of the project. The second part is dedicated to the legal framework and legal requirements of the DYNAMO technological solution and is addressed to its designers, developers and future deployers.

Table of Content

List of Tables

Chapter 1 Introduction

1.1 Deliverable positioning, scope, and objectives

Deliverable 1.3 ‘Ethical and Legal Protocol and Compliance Assessment’ corresponds to Task 1.4 ‘Ethical & Legal Aspects and Compliance Assessment’. Responsible for its preparation and delivery is the T1.4 Leader KEMEA that has undertaken the role of the project’s Ethics and Legal Advisor.

According to the Grant Agreement, T1.4 has two different objectives.

First, a thorough ethical evaluation of all project-related research activities needs to be conducted to ensure respect of the DYNAMO research for the applicable legal framework and ethical principles and to promote gender equality during the project’s lifespan. To this end, an internal guide (Ethics Guidelines) was issued within the first months of the project (M8 – May 2023) and was distributed to the Consortium to help the partners carry out research activities in an ethical and legally compliant manner. In the same spirit and to foster ethical and legal awareness, the content of the Ethics Guidelines was presented to the Consortium partners through a ‘Webinar on ethics’ organised by the Ethics and Legal Advisor on June 27, 2023.

Secondly, an analysis of the legal framework that applies to the DYNAMO solution needs to be conducted with emphasis on cybersecurity, data protection and artificial intelligence. The objective of this analysis is to ensure that the technological solution that is created during the lifetime of the project follows an ethics-, security- and privacy-by-design approach and will operate in conformity with the applicable EU and national laws.

To achieve the aforementioned goals the Ethics and Legal Advisor is in close collaboration with the DYNAMO Consortium by actively participating in the project meetings and communicating with the Consortium partners upon a partner’s request for guidance and assistance. In addition, since the commencement of the DYNAMO project, questionnaires related to the project’s identified ethics and legal issues were made available to the Consortium for the collection of feedback. The questionnaires are kept in a dedicated file of the project’s online repository in an online/modifiable form hence allowing modifications/updates to the responses whenever needed. Requests for review and update of the responses are made periodically (approx. every six months) by the Ethics and Legal Advisor to ensure proper monitoring during the lifetime of the project.

1.2 Structure of the deliverable

D1.3 is the official report of T1.4. In line with the objectives of each subtask, the deliverable aims to present the identified ethical and legal issues relating to the DYNAMO project and to assess the compliance (a) of the DYNAMO research and (b) of the DYNAMO technological solution with the existing ethical and legal framework.

The deliverable is structured as follows:

The first section constitutes the introduction which outlines the positioning, scope and objectives of the deliverable.

Sections 2 and 3 constitute the core of the deliverable.

The second section focuses on the DYNAMO research activities, the relevant ethical and legal issues, the risks that have been identified and the mitigating actions that need to be taken to ensure compliance of the research with the Horizon Europe standards, the ethical principles and the applicable legal framework. This section is an updated version of the internal guide (Ethics Guidelines).

The third section is focused on the DYNAMO technological solution, the applicable legal framework and the legal requirements that need to be defined for the solution to be designed, developed and deployed in conformity with the applicable regulatory framework. This section feeds T2.2 ‘User requirements elicitation and formalisation’ and the corresponding report D2.1.

The final section presents the concluding remarks.

Lastly, the Annex includes the internal guide that was prepared by the Ethics and Legal Advisor within the first months of the project, was distributed to the DYNAMO Consortium and was presented to the Consortium partners on June 27, 2023 through a dedicated ethics webinar.

Chapter 2 Research Ethics

This chapter is focused on the DYNAMO research activities and constitutes the updated version of the internal guide (Ethics Guidelines) which can be found in the Annex below.

During the preparation of the DYNAMO proposal, the internal ethics experts from KEMEA took into consideration the types of the DYNAMO research activities and conducted an initial ethics self-assessment which can be found under Section 4 Ethics Self-Assessment of the DYNAMO Grant Agreement. Based on this, the DYNAMO ethical issues are relating to:

- **humans** (participation of humans in research activities),
- **personal data** (processing of personal data as part of the research activities) and
- **artificial intelligence** (design, development and use of AI-enabled technologies as part of the project).

The Granting Authority assessed that the ethical issues listed in the self-assessment form are appropriately addressed in T1.4 'Ethical & Legal Aspects and Compliance Assessment' and decided that an additional Work Package with post-grant ethics requirements did not need to be set out for the DYNAMO project. The corresponding Deliverable 1.3, i.e., the present document, was deemed sufficient to collectively report on the project's compliance with the legal and ethical frameworks.

Apart from the aforementioned ethical issues, another common risk in research projects which could be also relevant to DYNAMO is that of **potential misuse of the research results**.

Therefore, five questionnaires were drafted (one for humans, two for personal data, one for artificial intelligence, and one for misuse) and were addressed to the Consortium partners aiming to collect valuable information from the Consortium and effectively prevent or mitigate the relevant risks.

Special reference is made to **gender equality and gender balance** as per the description of T1.4.

Through the Ethics Guidelines and the ethics webinar, the DYNAMO Consortium was familiarised with the project-related ethical and legal issues and the relevant risks, and the partners acting as lead researchers were informed of the ethics and legal requirements that must be met for the research activities to be carried out in compliance with the Horizon Europe standards, the ethical principles and the applicable legislation.

In the following sections of this chapter each issue is separately examined.

2.1 Humans

"Research with humans" refers to any research involving work with human beings, regardless of its nature or topic and irrespective of whether the participants are from or outside of the Consortium.

Where human beings are involved as participants in a research activity, the research must comply with ethical principles and applicable international, EU and national laws.

A dedicated questionnaire was made available to the Consortium aiming to collect feedback from all partners about their involvement in the project's research activities with human participants. The below activities represent most, if not all, of the DYNAMO activities involving human participants that will occur. Due to the nature of an evolving project, other (similar) research activities with human participants may occur during the project that have not yet been fully anticipated and thus have not been listed here; any extra activities involving human participants will fall within the categories of interviews/questionnaires/pilot demonstrations/workshops/events and will comply with the relevant sections of D1.3.

2.1.1 *The DYNAMO research activities with humans*

In DYNAMO the following activities involve human participants:

- Interviews:
  - T3.1 (Lead: UCC) interviews with IT and CTI experts in the consortium and the DYNAMO network
  - T3.2 (Lead: LAU, Contributors: FS and UCC) interviews with IT experts working in cyber crisis/cyber response (from the DYNAMO Consortium partners or other organisations) to understand human factors more relevant for the implementation of cyber response
  - T4.2 (Lead: LAU) interviews with cybersecurity experts from key sectors (energy, healthcare, and transportation) to understand how critical infrastructure organisations in Finland share Cyber Threat Intelligence (CTI)
  - T7.2 (Lead: TEC, Contributor: UCC) video interviews with DYNAMO researchers to raise awareness of the public about the project
- Online questionnaires/surveys:
  - T3.1 (Lead: UCC) online survey of the Consortium partners feedback on the definition and proposed framework
  - T3.2 (Lead: LAU) online societal impact questionnaire and online network resilience questionnaire with IT experts working in cyber crisis/cyber response (from the DYNAMO Consortium partners or other organisations) to understand human factors more relevant for the implementation of cyber response
- Trainings:
  - T3.2 (Lead: LAU, Contributor: UCC) practitioner and student feedback on BCM and CTI training
  - T3.3 (Lead: Fraunhofer, Contributor: UCC) practitioner and student feedback on BCM and CTI training
  - T6.3 (Lead: IRTSX, Contributor: UCC) end-user training sessions to educate stakeholders on general and sector-specific threats and their responsibilities as well as to provide training simulations for security practitioners
- Pilot demonstrations:
  - T6.2 (Lead: LAU, Contributor: UCC) sector specific (health, energy and maritime transportation) pilot demonstrations
  - T6.4 (Lead: UCC) cross-sector specific pilot demonstrations in the form of workshops, table-top exercises and simulations using DYNAMO and case study testing environments (along with evaluation workshops)
- Workshops/events:
  - T7.2 (Lead: TEC) workshops to raise awareness and foster acceptance among citizens, end-users, and stakeholders
  - T7.3 (Lead: TEC) workshops jointly with other EU projects and initiatives to foster scientific exchange among experts and practitioners
  - T7.3 (Lead: TEC) final dissemination event to present the results, exploiting synergies with other sector-related EU initiatives, and gathering representatives, industry, civil society, policy makers, academia, and EC officers

  - T3.2 (Lead: LAU) workshops to raise awareness, willingness and capabilities to share information, build and use cyber-threat intelligence and better respond through cyber/e-skills (technical, situation awareness or problem-solving skills)
- Questionnaires for collection of input and submission of project deliverables:
  - T1.4 (Lead: KEMEA) anonymous questionnaires addressed to the DYNAMO Consortium partners to collect feedback for the effective ethics management of the project
  - T1.5 (Lead: TEC) anonymous questionnaires addressed to the DYNAMO Consortium partners to collect feedback for the creation of the Data Management Plan
  - T2.1 & T2.2 (Lead: KEMEA) anonymous questionnaires (along with dedicated co-creation workshops) addressed to the DYNAMO Consortium partners to produce user requirements

2.1.2 Recruitment criteria

For compliance with the principles and the law to be achieved, respect for people and for human dignity and fair distribution of the benefits and burden of research must be ensured, and the values, rights and interests of the research participants must be protected. No discrimination of the participants is acceptable based on their age, race, sex, gender, disability, religion, beliefs, sexual orientation or on any other ground.

The participants are selected by the lead researchers based on (**inclusion criteria**):

- Their age (i.e., legal age required, only adults are eligible to participate);
- Their ability to provide consent;
- Their free will to participate;
- Their profession, scientific background, knowledge or experience on a specific field, if this is needed or recommended for the fulfilment of a project's task (e.g., IT experts working in cyber crisis/cyber response).

The DYNAMO Consortium does not recruit (**exclusion criteria**):

- Any person under the age of 18;
- Any person that is unable to give consent;
- Any person that has not followed the informed consent procedure or has withdrawn their consent.

2.1.3 Informed consent procedure for research participation

As a rule, human participation in the DYNAMO research activities is on a voluntary basis. Therefore, the informed consent procedure is followed prior to any research activity involving humans. The only exception is this of (anonymous) questionnaires addressed to the DYNAMO Consortium partners. In that case, the questionnaires are used solely to facilitate the collection of necessary input by the contributing partners as it is mandated by the Grant Agreement.

The lead researcher carrying out a research activity with humans informs the participants in advance through a detailed Information Sheet about the following:

- Who is organising and funding the research;
- A description of the project and its objectives;

- The type (e.g., interview, workshop, pilot demonstration, other) and a description of the specific research activity in which the participant is invited to participate;
- Where this research activity takes place;
- The date and duration of the research activity;
- The purpose of the specific research activity in which the participant is invited to participate;
- The criteria based on which the participant is invited to participate (recruitment criteria) and based on which she/he must be excluded (exclusion criteria);
- Any foreseeable risks, discomfort or disadvantages;
- Any benefits to the participant or to others which may be reasonably expected from the research;
- The voluntary character of the participation;
- The opportunity of the participant to ask questions and to withdraw at any time from the research activity without consequences;
- Any processing of personal data of the participants during the research activity (in that case detailed information of Article 13 GDPR will be provided through the Information Sheet or in other adequate ways) or the information about the anonymity of the participation if the collection of any personal information is considered unnecessary (e.g., anonymous online questionnaires/surveys). More details are provided below in sections 2.2.1.2 and 2.2.2.
- The contact details of the lead researcher (legal person responsible for the research activity and a natural person acting as contact point) in order to enable the participants ask questions and exercise their rights.

Prior to the start of a research activity, a copy of the Information Sheet is provided to the research participants in a language intelligible to them, in order for the lead researcher to be sure that they will be able to read the information therein at any time and that they will exercise their rights whenever they see the need to do so.

The consent of the participants is clearly and freely given through an Informed Consent Form (either in hard copy or online via tick boxes in case of online questionnaires/surveys) or orally before their participation and only after they have been fully informed about the specific conditions and characteristics of the research activity through the Information Sheet.

English is considered to be a language intelligible to all DYNAMO participants. However, in case the lead researcher identifies the need for translation of the documents, the Information Sheet and the Informed Consent Form will be translated in the native language of the participants.

The templates of Information Sheet and Informed Consent Form are kept in a dedicated file of the project's online repository in a modifiable form. The templates are modified by the lead researchers depending on the specific characteristics of each research activity.

2.1.4 Ethics approvals / opinions

Several EU member states and countries where EU-funded research takes place have established specific structures (Ethics Committees or other competent authorities) that, inter alia, issue ethics approvals and ethics opinions for research activities that involve humans. Such approvals are obtained prior to the start of the relevant research activities.

Based on the responses of the DYNAMO Consortium partners, only CERTH, LAUREA and UCC have established an internal Ethics Committee.

CERTH does not conduct research with humans, therefore approval/opinion is not required by its Ethics Committee. For the T4.1 'Cyber-threat intelligence gathering and extraction' research activities that are led by CERTH and involve data subjects, competent to issue an opinion is CERTH's Data Protection Officer (see below section 2.2.3).

LAUREA does not conduct research activities that require prior ethics committee approval. The opinion of LAUREA's RDI Coordinator has been consulted. All activities under T3.2 and T6.2 comply with the Finnish higher education ethics guidelines. Informed consent is asked from all questionnaire respondents, interviewees and workshop participants.

Training exercises in UCC were part of the teaching and learning programme for the students, with no ethics approval deemed necessary. Where ethical approval is required, the Social Research Ethics Committee (SREC) is the relevant ethics approval committee at UCC.

2.2 Personal data

The protection of natural persons in relation to the processing of personal data is a fundamental right. According to Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union (TFEU), everyone has the right to the protection of personal data concerning themselves.

During the lifetime of the DYNAMO project applicable are the General Data Protection Regulation (GDPR)[1] and the national data protection laws supplementing the EU Regulation. All data processing operations carried out during the project's lifespan must be in accordance with the EU and national legal framework on data protection.

As a preliminary remark, some important definitions are the following:

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others (Joint Controllers of Article 26 GDPR), determines the purposes (i.e., 'why?') and means (i.e., 'how?') of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[1] Regulation (EU) 2016/679 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)

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (i.e., in accordance with the controller's orders).[2]

Two dedicated questionnaires were made available to the Consortium aiming to collect feedback from all partners about their involvement in the project's data processing operations.

2.2.1 The DYNAMO data processing operations

The data processing operations in DYNAMO belong, based on their purpose, to four different categories:

2.2.1.1 Project coordination and management

Types of data: During the lifetime of the project and in the context of all Work Packages, the DYNAMO Consortium partners (controllers) process personal data of the personnel of the Consortium partners (data subjects) for the purpose of the proper coordination and management of the project including the necessary communication among the partners for the realisation of the project's tasks. Such personal data include names, email addresses, signatures, voice (if recorded during project meetings) and image (if captured during project meetings through video recordings) of the DYNAMO researchers.

Lawful basis: This processing is necessary for the performance of the DYNAMO Consortium Agreement and the DYNAMO Grant Agreement (Article 6(1)(b) GDPR).

Specifically, with respect to image/voice of the DYNAMO researchers that are recorded during project meetings, consent of the participants is asked prior to the start of the recording (Article 6(1)(a) GDPR).

Storage period: Personal data will be stored for 5 years after the end of the project in accordance with the DYNAMO Grant Agreement (mandatory record-keeping) for accountability reasons towards the Granting Authority.

Specifically with respect to image/voice of individuals that are recorded during project meetings, these types of personal data will be retained for the time stipulated in the DYNAMO Consortium Agreement that is necessary for the drafting of minutes. However, recordings of project meetings remain an exemption (for more information on the matter see the Project Handbook[3]).

Data transfers: No transfer outside of the EU or to international organisations is foreseen.

Rights of the data subjects: The data subjects have the rights stipulated by the GDPR (right to request information, right to access, right to rectification, right to erasure, right to restriction, right to data portability, right to lodge a complaint with a supervisory authority) and can exercise them by contacting the Data Protection Officer (DPO) of the controller or, in absence of a DPO, by contacting the controller itself.

The contact details of the partners' DPOs have been made available to the researchers in the relevant online questionnaire that is accessible to all Consortium partners through the project's online repository.

[2] GDPR, Article 4 (1) (2) (7) (8)

[3] The DYNAMO Project Handbook is an internal report drafted by Fraunhofer and TEC. It is available only to the DYNAMO Consortium.

2.2.1.2 Research activities that involve volunteers

Types of data: The lead researchers carrying out interviews, online surveys, trainings and pilot demonstrations (controllers) with volunteers (data subjects) may process personal data of the participants. The types of data may vary depending on the characteristics and purposes of the relevant tasks. The voice of the interviewees will be collected in the context of the WP3 interviews. Information about the exact types of data per research activity are included in the Information Sheet prepared by the lead researcher(s)/controllers.

The informed consent procedure is followed prior to the start of a research activity with volunteers. To this end, personal data of the participants are also collected by the lead researcher (controller), including the participants' name, company and signature (the latter only in case of Informed Consent Forms in hard copies).

Signatures will not be collected when the informed consent is obtained online through tick boxes (WP3 online questionnaires) or orally (WP3 interviews).

Lawful basis: In line with the voluntary character of the project's research activities, the processing of volunteers' personal data requires the consent of the data subjects (Article 6(1)(a) GDPR).

The consent is obtained through the informed consent procedure (see below section 2.2.2).

Storage period: Personal data will be stored for 5 years after the end of the project in accordance with the DYNAMO Grant Agreement (mandatory record-keeping) for accountability reasons towards the Granting Authority.

Specifically with respect to the voice of individuals that is recorded during the WP3 interviews, these types of personal data will be retained for the time needed for the transcription of the interviews. Only the introductory part of each recording will be retained for 5 years after the end of the project in accordance with the Grant Agreement (mandatory record-keeping) since it will contain information about the informed consent procedure provided by the interviewer and the explicit, clearly given consent of the interviewees.

Data transfers: No transfer outside of the EU or to international organisations is foreseen.

Rights of the data subjects: The data subjects have the rights stipulated by the GDPR (right to request information, right to access, right to rectification, right to erasure, right to restriction, right to data portability, right to lodge a complaint with a supervisory authority) and can exercise them by contacting the DPO of the controller or, in absence of a DPO, by contacting the controller itself.

The contact details of the lead researcher's DPO are made available to the research participants prior to the start of the research activity through the Information Sheet.

2.2.1.3 Research activities that involve individuals on a non-voluntary basis

As an exemption to the rule of informed consent, in case the consent of the data subjects cannot be obtained due to the nature of the data processing operation, another lawful basis must be sought by the lead researcher (controller). The personal data are processed solely for the DYNAMO scientific research purposes in compatibility with the purposes for which they were initially collected in accordance with Recitals 49 and 50 GDPR. Extended reference is made below in section 2.2.3

2.2.1.4 Dissemination and communication

Types of data:

1. Interviews and dissemination workshops or events:

Personal data of interviewees (data subjects) are processed by the interviewer TEC (controller) as part of in-person interviews with the DYNAMO researchers. These data include the name, company, image and voice of the interviewees. Personal data of attendees (data subjects) are processed by the workshop/event organiser TEC or any other partner (controller) as part of their registration and participation in workshops, conferences and similar dissemination events. These data include the name, email address, organisation, country of the attendees through online registration forms in case of online registration process. Their signatures may be collected through attendance lists in case of physical events. Image and voice of attendees are processed through photographs and videos.

The informed consent procedure is followed prior to the start of the aforementioned activities. To this end, personal data of the attendees are also collected by the event organiser (controller), including the participants' name, company and signature (the latter in case of Informed Consent Forms in hard copies – signatures will not be collected if the informed consent is obtained online through tick boxes). For the in-person interviews with the DYNAMO researchers, the interviewees give their consent orally after having received relevant information from the interviewer.

2. Website:

Personal data of the website users/visitors (data subjects) are processed by the DYNAMO website operator (controller) through the website's contact form. These data include the name, email address and company. Cookies are also processed.

Lawful basis: The processing of personal data requires the consent of the data subjects (Article 6(1)(a) GDPR).

1. Interviews, workshops and dissemination events:
   The consent of the interviewees and attendees is obtained through the informed consent procedure (see below section 2.2.2).
2. Website:
   The processing of data is carried out based on the consent of the website users/visitors. Information about the processing is provided through the Privacy Policy and Cookies Declaration/Policy of the DYNAMO website.

Storage period: Personal data will be stored for 5 years after the end of the project in accordance with the DYNAMO Grant Agreement (mandatory record-keeping) for accountability reasons towards the Granting Authority.

Specifically with respect to image and voice of individuals that is recorded during interviews or workshops/events and uploaded onto the DYNAMO website and the DYNAMO social media accounts, these types of personal data will be retained for the time the website and the social media accounts operate. Any other photos and video/audio recordings kept by the interviewer/workshop organiser (not uploaded) will be retained by the end of the DYNAMO project.

Data transfers: No transfer outside of the EU or to international organisations is foreseen. However, personal data uploaded online are made accessible to the general public worldwide.

Rights of the data subjects: The data subjects have the rights stipulated by the GDPR (right to request information, right to access, right to rectification, right to erasure, right to restriction, right to data portability, right to lodge a complaint with a supervisory authority) and can exercise them by contacting the DPO of the controller or, in absence of a DPO, by contacting the controller itself.

The contact details of the controller’s DPO are made available to the interviewees/attendees prior to the start of the relevant activity through the Information Sheet.

2.2.2 *Informed consent procedure for the processing of personal data*

As explained above, the DYNAMO research activities that involve humans are carried out on a voluntary basis and, consequently, the lawful basis for the processing of the volunteers’ (data subjects) personal data is their informed consent in accordance with Article 6(1)(a) GDPR.

‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[4]

The lead researcher (controller) carrying out research activities with volunteers and processing their personal data informs the participants in advance via a detailed Information Sheet about the following in accordance with Article 13 GDPR:

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the Data Protection Officer, where applicable;
- the types of personal data that will be processed;
- the purposes of the processing for which the personal data are intended;
- the legal basis for the processing;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 GDPR ‘Transfers subject to appropriate safeguards’ or 47 GDPR ‘Binding corporate rules’, or the second subparagraph of Article 49 ‘Derogations for specific situations’ (1) GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the data deletion procedure;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- the existence of automated decision-making, including profiling, if any, as well as the significance and the envisaged consequences of such processing for the data subject;
- the safeguards that will be implemented, including the implementation of the data minimisation principle.

[4] GDPR, Article 4(11)

A copy of the Information Sheet is provided to the research participants (data subjects) in a language intelligible to them, in order for the lead researcher (controller) to be sure that they will be able to read the information therein at any time and that they will exercise their rights whenever they see the need to do so.

The consent of the participants is clearly and freely given through an Informed Consent Form (either in hard copy or online via tick boxes in case of online questionnaires/surveys) or orally before their participation and the start of the relevant data processing operation and only after they have received the information of Article 13 GDPR through the Information Sheet.
With respect to the WP3 interviews (which are intended to be anonymous), the informed consent procedure will be followed orally. Prior to the start of the interview, the interviewer will start the recording by informing the interviewees about the processing of their voice, the purpose of the processing, the storage period, the rights of the data subjects according to the GDPR and will also give the contact details of the interviewer and of the DPO, if applicable, to enable the participants exercise their data protection rights. An Information Sheet with all this information will be sent to the interviewees if they express their wish to have it in writing (a relevant question will be asked by the interviewer).

English is considered to be a language intelligible to all DYNAMO participants. However, in case the lead researcher (controller) identifies the need for translation of the documents, the Information Sheet and the Informed Consent Form will be translated in the native language of the participants.

The templates of Information Sheet and Informed Consent Form are kept in a dedicated file of the project's online repository in a modifiable form. The templates are modified by the lead researchers (controllers) depending on the specific characteristics of each data processing operation.

2.2.3 Deviation from the informed consent procedure

As explained above, the rule in DYNAMO is that the data are obtained by the data subjects either for the performance of the Grant Agreement and the Consortium Agreement (Article 6(1)(b) GDPR) for the carrying out of research activities and dissemination activities with human participants based on their consent (Article 6(1)(a) GDPR).

In cases where the personal data are not obtained by the data subjects, Article 14 GDPR applies. Article 14(5)(b) GDPR stipulates that if the provision of information about the data processing proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) GDPR, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests (e.g., anonymisation, pseudonymisation, encryption), including making the information publicly available (e.g., through the controller's and/or the DYNAMO project's official websites).

Such data processing operations are carried out by CERTH as part of Task 4.1 'Cyber-threat intelligence gathering and extraction' given that the personal data processed through the relevant module (web and social media crawler) are not obtained by the data subjects and they are further processed for the DYNAMO scientific research purposes without the knowledge and, consequently, without the consent of the data subjects. Due to the nature of these data processing operations, the involved data subjects cannot be informed of the processing.

In accordance with Article 35(1)(2) GDPR, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. The controller shall seek the advice of the DPO, where designated, when carrying out a Data Protection Impact Assessment (DPIA).

Since the processing of personal data through crawlers constitutes systematic monitoring of a publicly accessible area (e.g., internet or social media) on a large scale, this may result in high risks to the rights and freedoms of the data subjects (Article 35(3)(c) GDPR). Therefore, CERTH has conducted a DPIA in collaboration with the DPO designated in the organisation. The opinion of the DPO is included in the DPIA.

The lawful basis confirmed by CERTH is that of legitimate interests of the controller based on Article 6(1)(f) GDPR in conjunction with Recital 49 GDPR where it is provided for that the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

In addition, the T4.1 data processing operations carried out by CERTH constitute further processing of previously collected data for purposes different to the ones for which the personal data were initially collected by the website and social media operators. Further processing for scientific research purposes is considered to be compatible with the initial purposes and lawful according to Recital 50 GDPR provided that appropriate safeguards are implemented by the controller such as encryption or pseudonymisation.

In line with Articles 14(5)(b) and 89(1) GDPR and as expressly mentioned in the DPIA, CERTH respects the data minimisation principle by redacting personal data that are not deemed necessary as well as it implements cryptographic techniques to protect the personal data processed through the cyber-threat intelligence gathering and extraction module. In addition, the information of Article 14 GDPR will be made publicly available through the official DYNAMO website[5] to enable the data subjects to exercise their rights (title of the notice to be added to the website: ‘DYNAMO Data Protection Notice of Article 14(5)(b) GDPR’).

Following the opinion of CERTH’s DPO as expressed in the DPIA, all potential risks have been identified, the implemented technical and organisational measures constitute appropriate safeguards that effectively minimise the identified risks and the T4.1 data processing operations can start.

[5] https://horizon-dynamo.eu/

2.3 Artificial Intelligence

2.3.1 *Definition of AI system*

From the Ethics Guidelines for Trustworthy AI issued by the European Commission's High-Level Expert Group on AI (https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai):

"Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data, and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimisation), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)".

From the latest version of the AI Act, approved by the European Parliament on 13 March 2024 (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf):

"'artificial intelligence system' (AI system) means a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

2.3.2 *Ethics-by-design approach in research*

The key requirements for a trustworthy AI were presented in the Ethics Guidelines for Trustworthy Artificial Intelligence of the High-Level Expert Group on AI (AI HLEG), made public on 8 April 2019 and verified in the European Parliament's Framework on ethical aspects of AI, robotics and related technologies on 29 September 2020.

Following various reports on the matter where it has been expressed the necessity for a harmonised regulatory framework on AI in the European Union, the proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) was issued on 21 April 2021[6]. According to Article 2(6) of the latest version of the AI Act, as approved by the European Parliament[7], *"this Regulation shall not apply to any research and development activity regarding AI systems"*. Hence, the relevant activities carried out in the context of scientific research projects are out of the AI Act's scope based on the current provisions.

Nevertheless, the latter shall not mean that no rules apply in research. Researchers involved in AI development must show respect for fundamental human rights. Therefore, an ethics-by-design

[6] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021 COM (2021) 206 final 2021/0106 (COD)

[7] Artificial Intelligence Act European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts

approach must be followed during the design, development and use of the DYNAMO AI-based (including machine learning, hereinafter referred to as 'ML') components.

This approach aims to ensure trustworthiness and conformity of the AI systems with the Charter of Fundamental rights of the European Union and the key requirements for trustworthy AI listed and described in the AI HLEG Ethics Guidelines which are as follows:

- **Human agency and oversight**
  - Respect for human autonomy by allowing humans to make informed decisions.
  - Proper oversight mechanisms (human-in-the loop, human-on-the loop, human-in-command approaches) to ensure that AI systems act as enablers for a democratic society and foster fundamental rights.

- **Technical robustness and safety**
  - Resilience to attack and security.
  - General safety by following a preventative approach to risks.
  - Accuracy to ensure that training data are up to date, of high quality, complete and representative of the environment (by also monitoring false positives, false negatives) and communication of the accuracy metrics.
  - Reliability of the system to operate based on its intended goals, fall-back plans and reproducibility and relevant verification methods e.g., through logging.

- **Privacy and data governance**
  - Respect to the fundamental rights of privacy and data protection.
  - Data governance through appropriate mechanisms (DPIA, DPO consultation, data minimisation, privacy by design and by default through anonymisation, pseudonymisation or encryption of personal data, security standards etc.).

- **Transparency**
  - Traceability mechanisms for documenting and monitoring the complete trajectory of the AI system, from design and development to deployment and usage.
  - Explainability, i.e., the ability to explain both the technical processes and the reasoning behind the predictions, recommendations or decisions made (opposite example: black boxes).
  - Communication to the users that they are interacting with an AI system and implementation of mechanisms to inform users about the purpose, criteria and limitations of the predictions, recommendations or decisions made.

- **Diversity, non-discrimination and fairness**
  - Inclusion and diversity. Avoidance of unfair bias through a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design, also including mechanisms that allow for the flagging of issues related to bias, discrimination or poor performance of the AI system. The continuation of unfair biases could lead to unintended (in)direct prejudice and discrimination against certain groups or people, potentially leading to prejudice and marginalisation.
  - Accessibility and universal design in a way that allows a user-centric approach and people to use AI products or services, regardless of their age, gender, abilities or characteristics. AI systems should consider universal design principles addressing the

widest possible range of users to enable equal access and active involvement of all people.
- Active participation of stakeholders affected by the AI system from its design and development and even after its deployment.

- **Societal and environmental well-being**
  - Environmental well-being. Operation of the AI system in the most environmentally friendly way possible during its lifecycle.
  - Impact on work and skills. AI systems to support humans in the working environment and aim for the creation of meaningful work. Provision of information to the workers about the AI system's operation and impact.
  - Impact on society and democracy. AI systems to benefit all human beings, including future generations, to maintain and foster democratic processes and to respect the plurality of values and life choices of individuals.

- **Accountability and auditability**
  - Auditability through accessible mechanisms for accountability that ensure an adequate possibility of redress by design in case unjust or adverse impacts occur.
  - Risk management that identifies and mitigates risks in a transparent way that can be explained to and audited by third parties, i.e., ability to report on actions or decisions that contribute to the AI system's outcome, and to respond to the consequences of such an outcome.[8]

2.3.3 *Ethics by design for AI in the DYNAMO project*

A dedicated questionnaire was made available to the Consortium aiming to collect feedback from the partners that design, develop and use AI-based tools about the efforts made for the ethical creation of these tools. The questionnaire is based on the key requirements for trustworthy AI and was ultimately completed by VST and CERTH for the AI-driven modules developed as part of WP4. The results can be found below.

2.3.3.1 WP3, T3.2 'AI-based self-healing disaster mitigation, response & recovery' (Lead: VST)

A prototype of a self-healing disaster mitigation, response and recovery solution will be developed. The solution is to be implemented through a domain independent mixed-initiative planning-scheduling and execution system. This system supports automation of business continuity plans. The AI solution allows the members of the organisation to interact with the automated processes and guide their behaviour when needed.

- ***Respect for human agency***: The system offers suggestions that are always confirmed and validated by humans (decision-makers). Hence, it can be confirmed that the AI system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects

[8] AI HLEG (2019), Ethics Guidelines for Trustworthy AI, available at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai and AI HLEG (2020), Assessment List for Trustworthy Artificial Intelligence (ALTAI), available at https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

individuals. Furthermore, the system does not affect the decision-making capabilities of its operators. Thus, it can be confirmed that end-users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives or take autonomous decisions about their lives. In addition, with respect to the potential risk of guided decision-making affecting operators' confidence or their dependency on the system, the AI system’s impact must be evaluated before releasing the product to potential future customers as well as it needs to be confirmed that the operators’ relationship to the system does not exceed their professional behaviour. The level of potential attachment needs to be reassessed.

- ***Security and resilience**:* Some measures to ensure robustness and safety in the AI system include rigorous input validation and sanitisation, and thorough model testing. Hence, it can be confirmed that the AI system design and implementation ensure technical robustness and safety. Furthermore, the AI system design and implementation should prioritise high-quality data, meticulous preprocessing, and thorough feature engineering. It is crucial to document and control the entire workflow, covering data processing, model architecture, and hyperparameters. Finally, it is crucial to implement rigorous unit and integration testing of the source code to ensure reproducibility and reliability of the AI system.
- ***Privacy and data governance**:* No personal data are processed by the system.
- ***Fairness and non-discrimination**:* The AI system is designed to avoid algorithmic bias, in input data, modelling and algorithm design. Furthermore, the AI system is designed to avoid historical and selection bias in data collection, representation and measurement bias in algorithmic training, aggregation and evaluation bias in modelling and automation bias in deployment. However, while algorithmic, historical or selection bias is not foreseen, the definitive answer to these questions requires more thorough assessment within T3.4. This assessment will take place after the requirements for the AI system are collected and during the design phase of the AI system. This is the time when the AI developer will be in a place to better justify that the system is designed to avoid algorithmic or any other types of bias. Moreover, the system design is based on the process and the role of its operator regardless of their personal specifications, hence, it can be used by various end-users with different abilities. This means that the AI system is designed so that it can be used different types of end-users with different abilities. Finally, it can be confirmed that the AI system does not have negative social impacts on the affected groups of individuals, including impacts other than those resulting from algorithmic bias or lack of universal accessibility. However, again, the definitive answer to this question requires more thorough assessment within T3.4. This assessment will take place after the requirements for the AI system are collected and during the design phase of the AI system. As regards potential negative discrimination against people on the basis of any grounds (e.g., sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation), this is out of the system’s scope and objectives, hence, such risks are not anticipated.
- ***Individual, and social and environmental well-being**:* This is out of the system’s scope and objectives; hence, any relevant risks are not anticipated.
- ***Transparency**:* The end-users will be aware that they are interacting with an AI system. Also, the purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed will be openly communicated to and understood by end-users and other stakeholders along with its possible consequences. These will be accomplished through the product description once the AI system is deemed ready to be put on the market. Furthermore, people can audit, query, dispute, seek to change or object to AI activities (human intervention) as the system provides only suggestions and the decisions are taken

by humans. Finally, via system settings and logs the AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit as well as it keeps records of the outputs produced and offers details about how the outputs are produced and on which reasons these were based.

- ***Accountability and oversight**:* With respect to accountability, the actors involved in the development or operation of the AI system should take responsibility for the way that these applications function and for the resulting consequences. To this end and since the system does not provide details of how potential ethically and socially undesirable effects will be detected, stopped, and prevented from reoccurring, a relevant disclaimer will be added explaining that the developers and operators take responsibility for any undesirable effects that cannot be anticipated at this stage. As for human oversight, the system provides graphical visualisation and interactive analysis, and the decisions are taken by humans, hence, humans are able to understand, supervise and control the design and operation of the AI-based system.

2.3.3.2 WP4, T4.3 ‘Advances AI-based analysis & correlation’ (Lead: VST)

The Cyber Knowledge Graph (CKG) is an AI-driven cyber security system that collects and correlates threat intelligence from various sources. It employs Natural Language Processing to extract knowledge from text, assess its relevance, and map it to ontology concepts. It also integrates graphical visualisation and interactive analysis allowing security analysts to query and analyse the data, enhancing their situational awareness. The CKG can be used as an extension to an Early Warning System or as a standalone search and analysis tool.

- ***Respect for human agency**:* The system offers suggestions that are always confirmed and validated by humans (decision-makers). Hence, it can be confirmed that the AI system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects individuals. Furthermore, the system does not affect the decision-making capabilities of its operators. Thus, it can be confirmed that end-users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives or take autonomous decisions about their lives. In addition, with respect to the potential risk of guided decision-making affecting operators' confidence or their dependency on the system, the AI system’s impact must be evaluated before releasing the product to potential future customers as well as it needs to be confirmed that the operators’ relationship to the system does not exceed their professional behaviour. The level of potential attachment needs to be reassessed.
- ***Security and resilience**:* Some measures to ensure robustness and safety in the AI system include rigorous input validation and sanitisation, and thorough model testing. Hence, it can be confirmed that the AI system design and implementation ensure technical robustness and safety. Furthermore, the AI system design and implementation should prioritise high-quality data, meticulous preprocessing, and thorough feature engineering. It is crucial to document and control the entire workflow, covering data processing, model architecture, and hyperparameters. Finally, it is crucial to implement rigorous unit and integration testing of the source code to ensure reproducibility and reliability of the AI system.
- ***Privacy and data governance**:* No personal data are processed by the system.
- ***Fairness and non-discrimination**:* The AI system is designed to avoid algorithmic bias, in input data, modelling and algorithm design. Furthermore, the AI system is designed to avoid historical and selection bias in data collection, representation and measurement bias in algorithmic training, aggregation and evaluation bias in modelling and automation bias in

deployment. However, while algorithmic, historical or selection bias is not foreseen, the definitive answer to these questions requires more thorough assessment within T4.3. This assessment will take place after the requirements for the AI system are collected and during the design phase of the AI system. This is the time when the AI developer will be in a place to better justify that the system is designed to avoid algorithmic or any other types of bias. Moreover, the system offers a visualisation tool to be used by security analysts. Nevertheless, it can be used by various end-users with different abilities. This means that the AI system is designed so that it can be used different types of end-users with different abilities. Finally, it can be confirmed that the AI system does not have negative social impacts on the affected groups of individuals, including impacts other than those resulting from algorithmic bias or lack of universal accessibility. However, again, the definitive answer to this question requires more thorough assessment within T4.3. This assessment will take place after the requirements for the AI system are collected and during the design phase of the AI system. As regards potential negative discrimination against people on the basis of any grounds (e.g., sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation), this is out of the system’s scope and objectives, hence, such risks are not anticipated.

- ***Individual, and social and environmental well-being:*** This is out of the system’s scope and objectives; hence, any relevant risks are not anticipated.
- ***Transparency:*** The end-users will be aware that they are interacting with an AI system. Also, the purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed will be openly communicated to and understood by end-users and other stakeholders along with its possible consequences. These will be accomplished through the product description once the AI system is deemed ready to be put on the market. Furthermore, people can audit, query, dispute, seek to change or object to AI activities (human intervention) as the system provides graphical visualisation and interactive analysis and the decisions are taken by humans. Finally, via system settings and logs the AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit as well as it keeps records of the outputs produced and offers details about how the outputs are produced and on which reasons these were based.
- ***Accountability and oversight:*** With respect to accountability, the actors involved in the development or operation of the AI system should take responsibility for the way that these applications function and for the resulting consequences. To this end and since the system does not provide details of how potential ethically and socially undesirable effects will be detected, stopped, and prevented from reoccurring, a relevant disclaimer will be added explaining that the developers and operators take responsibility for any undesirable effects that cannot be anticipated at this stage. As for human oversight, the system provides graphical visualisation and interactive analysis, and the decisions are taken by humans, hence, humans are able to understand, supervise and control the design and operation of the AI-based system.

2.3.3.3 WP4, T4.1 ‘Cyber-threat intelligence gathering and extraction’ (Lead: CERTH)

The Cyber-Threat Intelligence Extractor (CTI) is tool responsible for collection, extraction, analysis and correlation of CTI from both several external (i.e., online), as well as internal sources with the use of ML-based algorithms. CTI Extractor filters the collected data to avoid storing personal data leveraging rule-based techniques and extracts CTI from the collected sources using rule-based and ML-based techniques. The collected data are further analysed in order to identify possible correlations between the information collected both from external as well as internal sources. CTI Extractor utilises both simple and advanced correlations of threats.

- ***Respect for human agency**:* The AI system makes correlations. It cannot take decisions or actions and requires human oversight. The user is responsible to take decisions by utilising the information that the tool is providing. Hence, it can be confirmed that the AI system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects individuals. Furthermore, it can be confirmed that end-users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives or take autonomous decisions about their lives. Finally, it can be confirmed that end-users and others affected by the AI system are not subordinated, coerced, deceived, manipulated, objectified or dehumanised, nor are attached or addicted to the system and its operations.
- ***Security and resilience**:* It can be confirmed that the AI system design and implementation ensure technical robustness and safety. It also ensures accuracy, reproducibility and reliability. Multiple security measures that constitute appropriate safeguards are described in detail in the DPIA that has been conducted and approved by the DPO.
- ***Privacy and data governance**:* The AI system processes data in line with the requirements for lawfulness, fairness and transparency set in the national and EU data protection legal framework and the reasonable expectations of the data subjects. Also, the processing of personal data is carried out for specific purposes in accordance with the purpose limitation principle and for a specific period of time that is needed to achieve the defined purposes in accordance with the storage limitation principle. Technical and organisational measures are in place to safeguard the rights of data subjects (data minimisation and encryption). Security measures are also in place to prevent data breaches and leakages. All relevant information about the types of personal data, the lawful basis, the purposes, the storage period, the identified risks and the appropriate safeguards to minimise the risks is included in the DPIA that has been conducted and approved by the DPO.
- ***Fairness and non-discrimination**:* Discrimination parameters are not used. The types of personal data that are collected through the AI system to meet its intended purposes (IP addresses and email addresses) cannot lead to discrimination of the data subjects. In case any other personal data are collected incidentally during the operation of the tool, they are immediately redacted in accordance with the data minimisation principle. The system is designed to be used by cyber security experts and system and network admins.
- ***Individual, and social and environmental well-being**:* This is out of the system's scope and objectives; hence, any relevant risks are not anticipated.
- ***Transparency**:* The end-users will be aware that they are interacting with an AI system. Also, the purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed will be openly communicated to and understood by end-users and other stakeholders along with its possible consequences. Furthermore, people can audit, query, dispute, seek to change or object to AI activities (human intervention) given that the decisions are taken by humans. Finally, the AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit as well as it offers details about how the outputs are produced and on which reasons these were based. All information related to the above along with guidelines will be included in the relevant project deliverables and documentation.

- ***Accountability and oversight****:* With respect to accountability, the actors involved in the development or operation of the AI system should take responsibility for the way that these applications function and for the resulting consequences. The system provides details of how potential ethically and socially undesirable effects will be detected, stopped, and prevented from reoccurring. As for human oversight, the system only makes correlations. Humans are able to understand, supervise and control the design and operation of the AI-based system and are the ones responsible to take the decisions.

2.3.3.4 WP4, T4.4 'AI-based Predictive Analytics' (Lead: CERTH)

The Cyber-Attack Forecasting (CAF) is a tool that provides next-minute cyber-attack forecasts, by considering network traffic measurements.

- ***Respect for human agency****:* The AI system makes predictions. It cannot take decisions or actions and requires human oversight. The user is responsible to take decisions by utilising the information that the tool is providing. Hence, it can be confirmed that the AI system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects individuals. Furthermore, it can be confirmed that end-users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives or take autonomous decisions about their lives. Finally, it can be confirmed that end-users and others affected by the AI system are not subordinated, coerced, deceived, manipulated, objectified or dehumanised, nor are attached or addicted to the system and its operations.
- ***Security and resilience****:* It can be confirmed that the AI system design and implementation ensure technical robustness and safety. It also ensures accuracy, reproducibility and reliability. Multiple security measures that constitute appropriate safeguards are described in detail in the DPIA that has been conducted and approved by the DPO.
- ***Privacy and data governance****:* The AI system processes data in line with the requirements for lawfulness, fairness and transparency set in the national and EU data protection legal framework and the reasonable expectations of the data subjects. Also, the processing of personal data is carried out for specific purposes in accordance with the purpose limitation principle and for a specific period of time that is needed to achieve the defined purposes in accordance with the storage limitation principle. Technical and organisational measures are in place to safeguard the rights of data subjects (data minimisation and encryption). Security measures are also in place to prevent data breaches and leakages. All relevant information about the types of personal data, the lawful basis, the purposes, the storage period, the identified risks and the appropriate safeguards to minimise the risks is included in the DPIA that has been conducted and approved by the DPO.
- ***Fairness and non-discrimination****:* Discrimination parameters are not used. The types of personal data that are collected through the AI system to meet its intended purposes (IP addresses, email addresses) cannot lead to discrimination of the data subjects. In case any other personal data are collected incidentally during the operation of the tool, they are immediately redacted in accordance with the data minimisation principle. The system is designed to be used by cyber security experts and system and network admins.
- ***Individual, and social and environmental well-being****:* This is out of the system's scope and objectives; hence, any relevant risks are not anticipated.
- ***Transparency****:* The end-users will be aware that they are interacting with an AI system. Also, the purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed will be openly communicated to and understood by end-users and other

stakeholders along with its possible consequences. Furthermore, people can audit, query, dispute, seek to change or object to AI activities (human intervention) given that the decisions are taken by humans. Finally, the AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit as well as it offers details about how the outputs are produced and on which reasons these were based. All information related to the above along with guidelines will be included in the relevant project deliverables and documentation.

- ***Accountability and oversight**:* With respect to accountability, the actors involved in the development or operation of the AI system should take responsibility for the way that these applications function and for the resulting consequences. The system provides details of how potential ethically and socially undesirable effects will be detected, stopped, and prevented from reoccurring. As for human oversight, the system only makes predictions. Humans are able to understand, supervise and control the design and operation of the AI-based system and are the ones taking the decisions.

2.4 Potential misuse of research results

2.4.1 The notion of misuse

The European Commission has issued guidelines[9] in order to help all parties involved in Horizon projects take the necessary measures to avoid potential misuse of research findings. The main questions to understand the notion of misuse are the following:

- If materials/methods/technologies and knowledge involved or generated were modified or enhanced, could they harm humans, animals or the environment?
- What would happen if the materials/methods/technologies and knowledge involved or generated ended up in the wrong hands?
- Could the materials/methods/technologies and knowledge involved or generated serve purposes other than those intended? If so, would such use be unethical?

To identify any possible misuse, it is important to start by considering the risks associated with the research planned and any unethical ways in which the materials, methods, technologies and knowledge involved or generated could be used. The research most vulnerable to misuse is research that:

- provides knowledge, materials and technologies that could be channelled into crime or terrorism;
- could result in chemical, biological, radiological or nuclear weapons and the means for their delivery (not applicable to DYNAMO);
- involves developing surveillance technologies that could curtail human rights and civil liberties;
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

[9] European Commission, How to complete your ethics self-assessment (version 2.0), 13 July 2021, available at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf

2.4.2 Mitigation strategy

Some technologies, methods and knowledge that are generated or used during the DYNAMO research could be used for unintended malicious and unethical purposes despite the researchers' benign intentions.

The DYNAMO Consortium has adopted a mitigation strategy by following procedures and implementing measures to prevent potential misuse of the research findings. Such procedures and measures are the following:

- Deliverables that include sensitive information which could be misused if ended up in the wrong hands are disseminated only amongst the Consortium and the Granting Authority (SEN).
- Information that includes details on the technologies, methods, knowledge that could be misused is filtered prior to publications or dissemination events and is not communicated to the public. The Dissemination & Communication Leader (TEC) is in close collaboration with the Ethics and Legal Advisor (KEMEA) and the Project Coordinator in order to filter the project-related information that is planned to be made available to the public through public dissemination events or publications or through the DYNAMO website and social media accounts and remove any references that are likely to cause misuse of the research results.
- Sensitive information involved or generated during a project's task is available only between the WP Leader and the Task Leader and only to authorised personnel of these Consortium partners that have a need-to-know.
- The project's research activities that may involve technologies, methods or information likely to be misused are carried out in a controlled environment.
- Dummy data may be used wherever possible.
- The data minimisation principle is respected. If the processing of personal data is not necessary for the purposes of a research activity, then personal data are not collected (e.g., anonymous questionnaires and surveys).
- A DPIA of Article 35 GDPR has been conducted prior to these data processing operations that are likely to result in high risks for the rights and freedoms of the data subjects (see above section 2.2.3). The DPIA is reviewed periodically and will be updated if needed.
- Further to the DPIA, a Data Protection Notice of Article 14(5)(b) GDPR will be uploaded on the project's website to enable the data subjects to exercise their data protection rights (see above section 2.2.3).

2.5 Gender equality and gender balance

The European Commission is committed to promoting gender equality in research and innovation. To this end, a European Commission Gender Equality Strategy 2020-2025 has been established which sets out the EC's broader commitment to equality across all EU policies. Furthermore, the EU has a well-established regulatory framework on gender equality, including binding directives, which apply widely across the labour market including the research sector.

The 3 main levels at which gender equality is addressed in Horizon Europe are as follows:

- Having a Gender Equality Plan (GEP) in place is an eligibility criterion for certain categories of legal entities from EU countries and non-EU countries associated to Horizon Europe.

- The integration of a gender dimension into research and innovation content is a requirement by default that is evaluated under the excellence criterion during the proposal phase, unless the topic description explicitly specifies otherwise.
- Increasing gender balance throughout the programme is another objective, with a target of 50% women in Horizon Europe related boards, expert groups and evaluation committees, and gender balance among research teams.

Considering the above:

- The DYNAMO Consortium partners that have already internally established a GEP must carry out research in conformity with it.
- Gender dimension is an important aspect in security that involves integrating gender into research and innovation processes by analysing gender needs, attitudes, and behaviours to enhance knowledge and technologies. Given that DYNAMO is not a gender-dedicated project, the aforementioned aspect needs to be taken into account to the extent that this is relevant to the project’s needs and final results.
- All DYNAMO partners are encouraged to involve females in their research teams and to recruit female participants when carrying out research activities during the lifetime of the project in order to increase gender balance.

Chapter 3 Applicable legal framework and requirements

This chapter extends beyond the DYNAMO research and is focused on the EU ethical and legal framework that surrounds the DYNAMO technological solution and on the requirements that must be met for its ethical and lawful operation. The information included herein gives outputs to Task 2.2 'User requirements elicitation and formalisation'. In particular, the legal requirements that are derived from the applicable regulatory framework aim to form a part of the user and system requirements that have been collected by the DYNAMO technology providers and end-users and reported in D2.1 'End-User and System Requirements' (Lead: KEMEA).

The scope of DYNAMO is to combine the two fields of business continuity management (BCM) and cyber-threat intelligence (CTI) to generate a situational awareness picture for decision support across all stages of the resilience management life cycle (prepare, prevent, protect, response, recover). During the lifecycle of the DYNAMO project, professionals of different backgrounds collaborate with end-users to develop, improve, and combine specific tools into a single platform. The DYNAMO platform will enhance the capabilities of existing software tools and provide cyber security and resilience for critical entities, namely organisations in the critical **healthcare**, **energy**, and **transport (maritime)** sectors.

3.1 Cybersecurity

The current EU legislative framework applicable to digital products is based on Article 114 of the TFEU and is composed of several pieces of legislation, including laws on specific products and safety-related aspects or general legislation on product liability. This section presents the DYNAMO-related 'new entries' that form a part of the so called 'New Legislative Framework' (NLF) and have been issued to enhance the existing EU rules and ensure a high common level of cybersecurity as well as to harmonise cybersecurity requirements across the Union.

3.1.1 NIS 2 Directive – Scope and requirements

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.[10]

The NIS 2 Directive lays down:

(a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

[10] NIS 2 Directive, Article 1(1)

(b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;
(c) rules and obligations on cybersecurity information sharing;
(d) supervisory and enforcement obligations on Member States.[11]

It applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises, and which provide their services or carry out their activities within the Union.

Irrespective of the entity's size, it also applies to entities identified as critical entities under Directive (EU) 2022/2557[12] as well as to entities of a type referred to in Annex I or II[13], where:

(a) services are provided by:
    (i) providers of public electronic communications networks or of publicly available electronic communications services;
    (ii) trust service providers;
    (iii) top-level domain name registries and domain name system service providers;
(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;
(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;
(f) the entity is a public administration entity:
    (i) of central government as defined by a Member State in accordance with national law; or
    (ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

The essential and important entities must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of their network and information systems. When assessing the proportionality of the implemented measures, special

[11] Ibid., Article 1(2)
[12] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Article 2(1) according to which: 'Critical entity' means a public or private entity which has been identified by a Member State (deadline: 17 July 2026) in accordance with Article 6 of Directive 2022/2557 as belonging to one of the categories set out in the third column of the table in the Annex. The sectors are the following: Energy, Transport, Banking, Financial market infrastructure, Health, Drinking water, Waste water, Digital infrastructure, Public administration, Space, and Production, processing and distribution of food.
[13] According to Annex I of the NIS 2 Directive, the relevant entities belong to the following critical sectors: Energy, Transport, Banking, Financial market infrastructure, Health, Drinking water, Waste water, Digital infrastructure, ICT service management (business-to-business), Public administration, and Space. According to Annex II of the NIS 2 Directive, the relevant entities belong to the following critical sectors: Postal and courier services, Waste management, Manufacture, production and distribution of chemicals, Production, processing and distribution of food, Manufacturing, Digital providers, and Research.

emphasis shall be placed on the degree of the entity's exposure to risks, the entity's size, and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

The cybersecurity risk-management measures are based on an "all-hazards approach" that aims to protect network and information systems and the physical environment of those systems from various types of incidents. Therefore, the cybersecurity risk-management measures should also include measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 series.[14]

As a minimum, the measures shall include, indicatively, the following:

- policies on risk analysis and information system security;
- incident handling;
- business continuity, such as backup management and disaster recovery, and crisis management;
- supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- basic cyber hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- human resources security, access control policies and asset management;
- the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.[15]

As a prerequisite for the proper implementation of the cybersecurity risk-management measures and the proper monitoring of their efficacy, the management bodies of essential and important entities are required to follow training and shall encourage essential and important entities to offer similar training to their employees on a regular basis.[16]

By 17 October 2024, the Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive and shall apply those measures from 18 October 2024[17].

3.1.2 CER Directive – Scope and requirements

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive) lays down, among others, obligations on Member States to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions or economic activities within the scope of Article 114 TFEU are provided in an unobstructed manner in the internal market,

[14] NIS 2 Directive, Article 21(1), Recital 79
[15] Ibid., Article 21(2)
[16] Ibid. Article 20
[17] On 18 October 2024, Directive (EU) 2016/1148 (NIS Directive) is repealed.

in particular obligations to identify critical entities and to support critical entities in meeting the obligations imposed on them as well as obligations for critical entities aimed at enhancing their resilience and ability to provide services in the internal market.[18]

'Critical entity' means a public or private entity which has been identified by a Member State (deadline: 17 July 2026) as belonging to one of the categories set out in the third column of the table in the Annex. The sectors are the following: Energy, Transport, Banking, Financial market infrastructure, Health, Drinking water, Wastewater, Digital infrastructure, Public administration, Space, and Production, processing and distribution of food.[19]

'Essential service' means a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment.[20]

Member States must adopt a strategy for enhancing the resilience of critical entities[21] and must carry out a risk assessment (and update it whenever needed and at least every four years)[22].

Critical entities must conduct a risk assessment (and update it whenever needed and at least every four years) on the basis of the Member State risk assessments mentioned above by taking into account all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences.[23]

Following the outcomes of the risk assessment, the measures that need to be taken to ensure resilience of critical entities include measures that are necessary to:

- prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;
- ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;
- respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
- recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
- ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
- raise awareness about the risk reduction and climate adaptation measures and the adequate employee security management measures among relevant personnel, duly considering training courses, information materials and exercises.[24]

[18] CER Directive, Article 1(1)
[19] Ibid., Article 2(1), Annex
[20] Ibid., Article 2(5)
[21] Ibid., Article 4
[22] Ibid., Article 5
[23] Ibid., Article 12
[24] Ibid., Article 13

Furthermore, critical entities must notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Unless operationally unable to do so, critical entities must submit an initial notification no later than 24 hours after becoming aware of an incident, followed by a detailed report one month thereafter at the latest.

By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with the CER Directive. They shall apply those measures from 18 October 2024.

3.1.3 Cyber Resilience Act – Scope and Requirements

The Proposal for a Regulation of the European Parliament and of the Council on cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act) stipulates cybersecurity rules to ensure more secure hardware and software products, with fewer vulnerabilities, hence, more resilient against cyber-attacks.

The proposed Cyber Resilience Act lays down:

(a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;
(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;
(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;
(d) rules on market surveillance and enforcement of the above-mentioned rules and requirements.[25]

It applies to products with digital elements whose intended, or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.[26]

The security requirements relating to the properties of hardware and software products are as follows:

- Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;
- Products with digital elements shall be delivered without any known exploitable vulnerabilities;
- On the basis of the risk assessment referred to in Article 10(2) of the proposed Cyber Resilience Act and where applicable, products with digital elements shall:
  - be delivered with a secure by default configuration, including the possibility to reset the product to its original state;
  - ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;
  - protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms;

[25] Proposal for a Cyber Resilience Act, Article 1
[26] Ibid., Article 2(1). Exemptions are also listed in that Article – see paragraphs 2-5.

- protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user;
- report on corruptions;
- process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');
- protect the availability of essential functions, including the resilience against and mitigation of denial-of-service attacks;
- minimise their own negative impact on the availability of services provided by other devices or networks;
- be designed, developed and produced to limit attack surfaces, including external interfaces;
- be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
- provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;
- ensure that vulnerabilities can be addressed through security updates, including, where applicable, automatic updates and the notification of available updates to users;[27]
- take into account the outcome of the cybersecurity risk assessment during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.[28]

The vulnerability handling requirements addressed to the manufacturers of software and hardware products are as follows:

- identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;
- in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;
- apply effective and regular tests and reviews of the security of the product with digital elements;
- once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;
- put in place and enforce a policy on coordinated vulnerability disclosure;
- take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;
- provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

[27] Proposal for a Cyber Resilience Act, Annex I

[28] Ibid., Article 10(2)

- ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.[29]

Further to above, the following requirements are addressed to the manufacturers, aiming to demonstrate fulfilment of their legal obligations and compliance of the products with the applicable EU law:

- Technical documentation must be drawn up, providing information on the design, manufacture, and operation of a product and containing all the details necessary to demonstrate the product conforms to the applicable requirements. A cybersecurity risk assessment of Article 10 of the proposed Cyber Resilience Act must be included in the technical documentation.[30]
- A conformity assessment must be conducted to demonstrate whether specified requirements relating to a product have been fulfilled. Third parties must be involved in the process in case of specific types of critical products.[31] The conformity assessment procedures are described in detail in Annex VI of the proposed Cyber Resilience Act.
- The EU declaration of conformity (DoC) is a mandatory document that the manufacturer (or the authorised representative) needs to sign to declare that the product complies with the EU requirements. By signing the declaration, the manufacturer takes full responsibility for the product’s compliance with the applicable EU law.[32] The required content of the DoC is presented in Annex IV of the proposed Cyber Resilience Act.
- The CE marking obligation remains and is subject to the general principles stipulated in Article 30 of Regulation (EC) 765/2008.[33]

3.2 Personal data protection

The protection of natural persons in relation to the processing of personal data is a fundamental right. According to Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) TFEU, everyone has the right to the protection of personal data concerning themselves.

In cases where personal data are processed as part of the development (e.g., training, validation and testing data) and/or the deployment of a technological solution, such processing is subject to strict requirements.

3.2.1 General Data Protection Regulation (GDPR) – Scope and requirements

After having taken into consideration the need for reform of European data protection law as a contribution by the European Union to the global debate on adequately protecting privacy in a digital world, the European Union has legislated on the protection of natural persons with respect to the processing of personal data and on the free movement of such data by issuing Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

[29] Ibid., Annex I
[30] Ibid., Article 23, Annex V, Article 10
[31] Ibid., Article 24, Recital 45
[32] Ibid., Article 20
[33] Ibid., Article 22

GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. It also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[34]

Prior to the presentation of the GDPR requirements and as a prerequisite for compliance with them, the roles (and, consequently, the responsibilities) need to be clearly identified. A controller is a natural or legal person that determines the purposes and means of the processing. If more entities decide why and how a data processing operation is carried out, these are joint controllers of Article 26 GDPR and need to sign a joint controllership agreement. If an entity is mandated by a controller to carry out the processing on its behalf, that entity is a processor, a controller-processor agreement of Article 28(3) GDPR needs to be signed between the parties and the processor must not process those data except on instructions from the controller as they are defined in their agreement.

The main requirements are the following, starting with the GDPR principles:

Principles (key requirements) [35]	
Lawfulness, fairness and transparency	Personal data must be processed in a lawful, fair and transparent to the data subject manner.
Purpose limitation	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal data must be accurate and kept up to date. Any inaccurate data must be erased or rectified without delay.
Storage limitation	Personal data must be stored for no longer than necessary for the purposes for which they were collected.
Integrity and confidentiality	Appropriate technical and organisational safeguards must be implemented that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology.
Accountability	Necessary documentation must have been put in place to prove compliance of the data controller with the aforementioned requirements.

Table 1 - GDPR Principles

For the data processing operations to be lawful, these must be based on a lawful basis from the ones listed in Article 6 GDPR. The lawful bases most relevant to the DYNAMO platform are:

- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (most relevant to public entities and private entities acting on their behalf) according to Article 6(1)(e) GDPR;

[34] Ibid., Article 3(1)(2)
[35] Ibid., Article 5

- Legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (applicable only to private entities) according to Article 6(1)(f) GDPR.

The legitimate interests of the controller are explicitly justified in Recital 49 GDPR where it is stipulated that the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by CERTs, CSIRTs, by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.

The designation of a Data Protection Officer within the controller is highly recommended (in cases where this is not expressly mandated by the GDPR).

Technical and organisational measures including anonymisation, pseudonymisation or encryption of personal data as well as security measures must be implemented by the controller, ensuring also respect to the principles of data minimisation and privacy by design and by default.[36]

In cases where personal data are not obtained by the data subjects, apart from the implementation of appropriate safeguards, the information about the data processing operations (including all information of Article 14 GDPR) must be made publicly available to enable the data subjects to be informed of the processing and exercise their data protection rights. The uploading of a relevant Data Protection Notice on the website of the controller is an advisable way to fulfil that requirement.

In cases where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in high risks to the rights and freedoms of the data subjects, the controller must conduct a data protection impact assessment of Article 35 GDPR prior to the start of the data processing operations. The DPIA must be reviewed and updated periodically in collaboration with the designated DPO.

A record of the processing operations must be maintained by the controller according to Article 30 GDPR.

In case of a data breach, specific procedures need to be followed by the controller as described in Articles 33 and 34 GDPR. If the data breach is identified by a processor, the controller must be notified without undue delay.

3.3 Artificial Intelligence

The ethical and legal framework on AI constitutes a ground-breaking initiative of the EU legislator in an attempt to follow the rapid technological developments to the biggest extent possible, shape the digital future and smoothly incorporate AI in society. The framework on AI aims to prioritise fundamental rights and foster trust of the potentially affected persons during the design, development and use of AI systems until their decommissioning.

[36] See indicatively Articles 32, 24, 25 GDPR.

Since the DYNAMO platform is formed, among others, of AI-enabled modules, specific requirements must be met during design, development and deployment.

3.3.1 Ethics Guidelines for Trustworthy Artificial Intelligence

As mentioned previously, the AI HLEG made public on 8 April 2019 the Ethics Guidelines for Trustworthy AI.

The seven key requirements introduced in the guidelines (for more details see section 2.3.2) are mainly based on the Charter of Fundamental Rights of the European Union. A trustworthy AI system is designed and operates in compliance with applicable laws (lawful), it respects ethical standards and ethical values (ethical) and it ensures technical robustness, safety, accuracy and resilience by design (robust).

3.3.2 Artificial Intelligence Act – Scope and requirements

In 2021 the Commission proposed the first comprehensive regulatory framework on AI, which addresses the risks of AI applications and positions Europe to play a leading role globally. The EU Regulation on AI (AI Act) was formally approved by the European Parliament on March 13, 2024.[37] Following a transition period, it is estimated to be enforced in 2025. The AI Act puts the human in the centre (human-centred approach) and is a horizontal regulation, applicable to AI systems of all sectors which are classified according to the risk they are posing to the affected persons (risk-based approach). As in the GDPR, the AI Act's territorial scope extends beyond the EU to providers placing on the market or putting into service AI systems in the EU irrespective of whether they are established within the Union or in a third country as well as to providers and deployers of AI systems that are located in a third country where the outputs (i.e., predictions, recommendations or decisions) produced by the AI system are used in the EU.

It is worth repeating at this point that the AI Act is not applicable in case of AI systems specifically developed for the sole purpose of scientific research and development[38] (such as in DYNAMO where the produced platform is planned to be used at TRL5). However, under all circumstances, any research and development activity should be carried out in accordance with the Charter of Fundamental Rights of the European Union[39] and the AI HLEG Ethics Guidelines presented previously. Therefore, the obligations stipulated in the AI Act are more relevant in case of further development of the DYNAMO platform and must be fulfilled prior to its placement on the market.

In line with the risk-based approach, the EU legislator deemed necessary that AI systems that present a high risk to the rights and freedoms of individuals (high-risk AI systems) will be subject to the most stringent rules.

Amongst the categories of high-risk AI systems listed in Annex III of the AI Act[40], are also the ones related to Critical Infrastructure, i.e., AI systems intended to be used as safety components in the

[37] Artificial Intelligence Act European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts available at https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html

[38] AI Act, Article 2(6)

[39] Ibid., Recitals 1, 2

[40] Ibid., Annex III 'High-risk AI systems referred to in Article 6(2)'

management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating or electricity.

The obligations for the providers of high-risk AI systems *inter alia* include:

- Risk management system[41] and quality management system[42] (establishment, implementation, documentation and maintenance).
- Data governance for the training, validation and testing data, including bias mitigation. Training, validation and testing datasets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose.[43] It is highly recommended that the DYNAMO partners developing AI-enabled tools consult the 'Self-assessment guide for artificial intelligence (AI) systems' which was issued by the French Data Protection Authority (CNIL)[44].
- Preparation, maintenance and update of technical documentation.[45]
- Record-keeping through automatic recording of events (logs) during the design and development phases to ensure a level of traceability of the AI system's functioning that is appropriate to its intended purpose.[46]
- Transparency and provision of information to the deployers, including clear information about the system's characteristics, capabilities and limitations of performance (e.g., intended purpose, accuracy metrics, robustness, cybersecurity, any known or foreseeable circumstances that could have an impact on the expected level of accuracy, robustness and cybersecurity, any known or foreseeable circumstances that could lead to risks to health, safety and fundamental rights, information to enable the deployers to interpret the system's outputs and use the AI system properly), pre-determined changes to the system described in the initial conformity assessment, the human oversight measures, the computational and hardware resources needed and the expected lifetime of the system along with any necessary maintenance and care measures to ensure its proper functioning.[47]
- Human oversight measures which are either implemented by design (if technically possible) or can be implemented by the deployer of the AI system to prevent or minimise the risks to health, safety or fundamental rights that may emerge. The persons to whom human oversight is assigned must fully understand the capabilities and limitations of the system, remain aware of automation bias, be able to interpret the outputs of the system, be able to decide when to use or not use the outputs of the system, as well as be able to intervene or stop the system through a 'stop' button, or similarly, that allows the system to come to a halt in a safe state.[48]
- Appropriate level of accuracy, robustness and cybersecurity by design and during the system's development in a way that clarifies to the user the levels of accuracy and the relevant accuracy metrics, ensures resilience of the system with respect to errors, faults or inconsistencies that may occur within the system or the environment in which the system operates and ensures resilience of the system as regards malicious attempts by unauthorised third parties to modify their use or performance by exploiting the system vulnerabilities.[49] It is

[41] Ibid., Article 9
[42] Ibid., Article 17
[43] Ibid., Article 10
[44] See https://www.cnil.fr/en/self-assessment-guide-artificial-intelligence-ai-systems.
[45] Ibid., Article 11
[46] Ibid., Article 12, Article 20
[47] Ibid., Article 13
[48] Ibid., Article 14
[49] Ibid., Article 15

highly recommended that the DYNAMO partners developing AI-enabled tools consult the 'Multilayer Framework for Good Cybersecurity Practices for AI', which was issued by the European Union Agency for Cybersecurity (ENISA) in June 2023[50].

- Making available of the provider's contact details on the AI system, packaging or accompanying documentation.[51]
- Conducting of a conformity assessment before specific types of high-risk AI systems are placed on the market or put into service where compliance with all aforementioned obligations is demonstrated.[52]
- Drafting of a relevant EU declaration of conformity in a timely manner.[53]
- Affixing of the "CE marking" to the AI system.[54]
- Compliance with registration obligations.[55]
- Implementation of corrective actions to bring the AI system in conformity with the AI Act or to withdraw, disable or recall the AI system if needed and provision of information to the distributors, deployers and importers.[56]
- Demonstration of conformity upon a reasoned request of a national competent authority.[57]
- Ensuring that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.[58]

The obligations for the deployers of high-risk AI systems *inter alia* include[59]:

- Implementing appropriate technical and organisational measures to ensure that the AI system is used in accordance with the instructions of use accompanying the AI system.
- Assigning the human oversight of the AI system to natural persons with the necessary competence, training, authority and support.
- Informing, without undue delay, the provider or distributor and relevant market surveillance authority[60] and suspending the use of the system when they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk[61].
- Ensuring, if they control input data, that the data is relevant and sufficiently representative in light of the purpose of the AI system.
- Keeping the logs automatically generated by, to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in applicable Union or national law.
- Conducting a Data Protection Impact Assessment of Article 35 GDPR (if required).

[50] See https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai.
[51] Ibid., Article 16(b)
[52] Ibid., Article 16(f), Article 43
[53] Ibid., Article 16(g), Article 47
[54] Ibid., Article 16(h), Article 48
[55] Ibid., Article 16(i), Article 49(1)
[56] Ibid., Article 16(j), Article 20
[57] Ibid., Article 16(k)
[58] Ibid., Article 16(l)
[59] Ibid., Article 26
[60] Ibid., Article 3 point 26 where it is defined that "'market surveillance authority' means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020".
[61] Ibid., Article 79(1) where it is defined that "AI systems presenting a risk shall be understood as a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to fundamental rights of persons are concerned".

- Conducting a fundamental rights impact assessment[62] (recommended even in cases where it is not mandated by law).

3.3.3 Other relevant pieces of legislation in progress

On 28 September 2022, the Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence ("AI Liability Directive") was published.[63] The proposed AI Liability Directive complements the AI Act by introducing a new liability regime that ensures legal certainty, fosters consumer trust in AI, and assists consumers when making liability claims for damage caused by AI-enabled products and services. Its purpose is to harmonise non-contractual fault-based liability rules, in order to ensure that persons claiming compensation for damage caused to them by an AI system enjoy a level of protection equivalent to that enjoyed by persons claiming compensation for damage caused without the involvement of an AI system.[64] The proposed AI Liability Directive applies to AI systems that are available on the EU market or operating within the EU market.

Alongside the AI Act, the Council of Europe (CoE) Draft Framework Convention on AI, Human Rights, Democracy and the Rule of Law was finalised on March 14, 2024, by the Committee on Artificial Intelligence (CAI)[65] and aims to be a global instrument attractive to as many countries as possible from all regions of the world. The purpose of the Draft Convention is to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law.[66] However, considering that various changes have been made to its content from the beginning of this effort and the official version has not been released to the public, a final and complete opinion cannot be provided.

3.4 DYNAMO legal requirements

This section receives input from the previous sections 3.1,3.2 and 3.3 and presents the key DYNAMO legal requirements as they emerge from the current ethical and legal framework.

The objective is that the legal requirements will be taken into consideration for the ethical, legal and secure creation and operation of the DYNAMO platform and its components by the end of the project and they will turn into system requirements (to the extent possible). For the selection of the requirements listed below we took into consideration that the platform is planned to be used at TRL5.

[62] Ibid., Article 27

[63] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final. See also European Commission, Impact assessment report accompanying the document: Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, SWD (2022) 319 final and European Parliament, EPRS, Artificial intelligence liability directive, Briefing, February 2023.

[64] Proposal for an AI Liability Directive, Recital 7. See also Recital 9: "Such harmonisation should increase legal certainty and create a level playing field for AI systems, thereby improving the functioning of the internal market as regards the production and dissemination of AI-enabled products and services".

[65] Committee on Artificial Intelligence (CAI), Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (18 December 2023) available at https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043. This is the latest version made available to the public. The Framework Convention was finalised on March 14, 2024, and the draft text will be referred to the Committee of Ministers for adoption and opened for signature at a later stage.

[66] Ibid., Article 1(1)

The fulfilment of the selected requirements will constitute a solid basis for the further development of the platform in compliance with the applicable regulatory framework prior to its ultimate placing on the market.

It needs to be highlighted that prior to the placing of the DYNAMO platform in the market, the legislative developments must be considered, and all actors involved (DYNAMO developers, DYNAMO critical entities) will need to carefully study the applicable laws at EU and national level to ensure conformity with their obligations.

At all phases, the smooth collaboration among technology providers, end users and legal experts is critical for the delivery of a technological solution that will be secure, useful and compliant with the law.

Category	Description
CS[67]-01	Conducting a cybersecurity risk assessment and update it when needed (e.g., when becoming aware of new vulnerabilities)* *Collaboration is needed between developers and critical entities, i.e., end users.
CS-02	Implementing cybersecurity risk-management measures based on an "all-hazards approach" to protect network and information systems and the physical environment of those systems from various types of incidents (system failures, human error, malicious acts or natural phenomena)[68]
CS-03	Following training to ensure proper implementation of the cybersecurity risk-management measures and the proper monitoring of their efficacy
CS-04	Protecting the availability of essential functions, including the resilience against and mitigation of denial-of-service attacks
CS-05	Implementing secure by default configuration, including the possibility to reset the product to its original state
CS-06	Protecting from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems
CS-07	Protecting the integrity of stored, transmitted or otherwise processed data, commands, programs and configuration against any manipulation or modification not authorised by the user
CS-08	Protecting the confidentiality of stored, transmitted or otherwise processed data, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms
CS-09	Designing, developing and producing the technological solution in a proper way to limit attack surfaces, including external interfaces
CS-10	Designing, developing and producing the technological solution in a proper way to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques
CS-11	Minimising the technological solution's own negative impact on the availability of services provided by other devices or networks
CS-12	Providing security-related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions
CS-13	Reporting incidents, including reporting on corruptions of data (e.g., theft, extortion, bribery)
CS-14	Ensuring proper vulnerability handling

[67] CS stands for 'Cybersecurity'

[68] See above section 2.1.1 for more information about the indicatively listed risk-management measures.

CS-15	Identifying and documenting vulnerabilities and components contained in the technological solution
CS-16	Remediating vulnerabilities and ensuring that they can be addressed through security updates, including, where applicable, automatic updates and the notification of available updates to user
CS-17	Delivering the technological solution without any known exploitable vulnerabilities
CS-18	Applying effective and regular tests and reviews of the security of the technological solution
CS-19	Drawing up technical documentation (including therein the cybersecurity risk assessment) providing information on the design, manufacture, and operation of the technological solution and containing all the details necessary to demonstrate the solution conforms to the applicable requirements
PD[69]-20	Identifying the roles in the processing (controller, joint controllers, processor, third party etc) and consulting the DPO (if applicable)
PD-21	Processing personal data in a lawful, fair and transparent to the data subject manner based on a lawful basis (legitimate interests of the controller or public security)
PD-22	Processing personal data for specified, explicit and legitimate purposes and not further processing in a manner that is incompatible with the intended purposes
PD-23	Ensuring that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
PD-24	Protecting the integrity of stored, transmitted or otherwise processed personal data, against any manipulation or modification not authorised by the user
PD-25	Protecting the confidentiality of stored, transmitted or otherwise processed personal data, such as by pseudonymising, encrypting or anonymising relevant data at rest or in transit by state-of-the-art mechanisms
PD-26	Storing personal data for no longer than necessary for the purposes for which they were collected
PD-27	Applying systematic reviews to ensure that personal data are accurate and kept up to date and erase or rectify inaccurate data without delay
PD-28	Keeping records of the processing operations
PD-29	Conducting a data protection impact assessment prior to the start of the processing if the processing may result in high risks to the rights and freedoms of the data subjects and update it when needed
PD-30	Making publicly available the information about the processing by including all information of Article 14 GDPR (e.g., through the official website of the controller)
PD-31	Having a mechanism to report data breaches timely
AI-32	Implementing human oversight by design (i.e., human as the final decision-maker)
AI-33	Implementing human intervention by design (i.e., ability to intervene, pause or stop the system via a ‘stop’ button or similarly)
AI-34	Training the individuals to whom human oversight is assigned
AI-35	Record-keeping through automatic recording of events (logs) to ensure a level of traceability of the AI system’s functioning that is appropriate to its intended purpose
AI-36	Having the ability to explain both the technical processes and the reasoning behind the predictions, correlations and recommendations made by the AI system (explainability)
AI-37	Avoiding unfair bias both regarding the use of input data as well as for the algorithm design, also including mechanisms that allow for the flagging of issues related to bias, discrimination or poor performance of the AI system
AI-38	Ensuring proper data governance for the training, validation and testing data, including bias mitigation (datasets shall be relevant, sufficiently representative, and to the best

[69] PD stands for ‘Personal Data’

	extent possible free of errors, by also monitoring false positives and false negatives, and complete in view of the intended purpose)
AI-39	Ensuring technical robustness and security by following a proactive and 'all-hazards' approach to risks (see also the CS requirements above)
AI-40	Ensuring resilience to attacks (see also the CS requirements above)
AI-41	Ensuring reliability of the AI system to operate based on its intended goals, fallback plans and reproducibility and relevant verification methods (see also the CS requirements above)
AI-42	Communicating to the users the system's characteristics, capabilities and limitations of performance, including the intended purpose, accuracy metrics and any known or foreseeable circumstances that could lead to risks to fundamental rights or could have an impact on the expected level of accuracy, robustness and cybersecurity
AI-43	Ensuring active participation of stakeholders affected by the AI system from its design and development (and even after its deployment)
AI-44	Processing personal data in line with the GDPR (see also the PD requirements above)
AI-45	Preparing, maintaining and updating technical documentation

Table 2 - DYNAMO legal requirements

Chapter 4 Summary and Conclusion

The present deliverable includes the ethical and legal aspects of the DYNAMO project, and its purpose is twofold. First, it aims to assess and ensure compliance of the DYNAMO research with the Horizon Europe standards, the applicable laws and the ethical principles. Secondly, it aims to assess and ensure compliance of the DYNAMO technological solution with the relevant applicable and upcoming EU legislation.

As a result, the first main part of this document is dedicated to the description and analysis of the ethical and legal issues relating to the research activities. Extended information was provided about human participation, personal data, artificial intelligence, potential misuse of the research results and gender equality and balance. The types of activities, the risks, the measures for their mitigation and the procedures that are followed by the DYNAMO Consortium were explained.

The second main part is focused on the analysis of the ethical and legal framework and the consequent requirements that apply to the DYNAMO solution. Therefore, the (existing and upcoming) regulatory framework on cybersecurity, personal data protection and artificial intelligence along with guidelines issued by official bodies were presented and the main legal requirements that emerge from them were listed to ensure that an ethics, security- and privacy-by-design approach will be followed, and that the DYNAMO platform will be developed and used in compliance with the regulatory framework.

It is worth mentioning that at this stage of the DYNAMO project, our work is based on the current legislative developments, and since some legislations are still in progress (Cyber Resilience Act, AI Liability Directive, AI Act approved by the European Parliament and not yet issued), we are committed to closely monitoring them for updates.

The Ethics and Legal Advisor will continue to be in close collaboration with the DYNAMO Consortium and provide guidance and assistance. The ethics questionnaires that have been drafted and completed by the DYNAMO Consortium partners are kept in a dedicated file of the project's online repository in an online/modifiable form hence allowing modifications/updates to the responses whenever needed. Requests for review and update of the responses are made periodically (approximately every six months) by the Ethics and Legal Advisor to ensure proper monitoring during the lifetime of the project.

Chapter 5 List of Abbreviations

Abbreviation	Translation
AI	Artificial Intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
BCM	Business Continuity Management
CER	Critical Entities' Resilience
CERTH	Centre for Research and Technology Hellas (Consortium partner)
CERTs	Computer Emergency Response Teams
CKG	Cyber Knowledge Graph
CoE	Council of Europe
CSIRTs	Computer Security Incident Response Teams
CTI	Cyber-Threat Intelligence
DoC	Declaration of Conformity
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
FS	Factor Social – Consultoria em Psico – Sociologia e Ambiente Lda (Consortium partner)
GDPR	General Data Protection Regulation
GEP	Gender Equality Plan
IRTSX	Institut de Recherche Technologique System X (Consortium partner)
KEMEA	Kentro Meleton Asfaleias (Consortium partner)
LAU	Laurea University of Applied Sciences (Consortium partner)
ML	Machine Learning
NIS	Network Information System
SREC	Social Research Ethics Committee

TEC	Technikon Forschungs- und Planungsgesselschaft mbH (Consortium partner)
TFEU	Treaty of the Functioning of the European Union
TRL	Technology Readiness Level
UCC	University College Cork (Consortium partner)
VST	VisionSpace Technologies GmbH (Consortium partner)

Chapter 6 Bibliography

[1] AI HLEG, Ethics Guidelines for Trustworthy AI, 8 April 2019, available at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[2] AI HLEG (2020), Assessment List for Trustworthy Artificial Intelligence (ALTAI), 17 July 2020, available at https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[3] CNIL, Self-assessment guide for artificial intelligence (AI) systems, available at https://www.cnil.fr/en/self-assessment-guide-artificial-intelligence-ai-systems

[4] Committee on Artificial Intelligence (CAI), Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (18 December 2023) available at https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[6] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

[7] European Commission, How to complete your ethics self-assessment (version 2.0), 13 July 2021, available at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf

[8] European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022)

[9] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021 COM (2021) 206 final 2021/0106 (COD)

[10] European Commission, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act) COM/2022/454 final

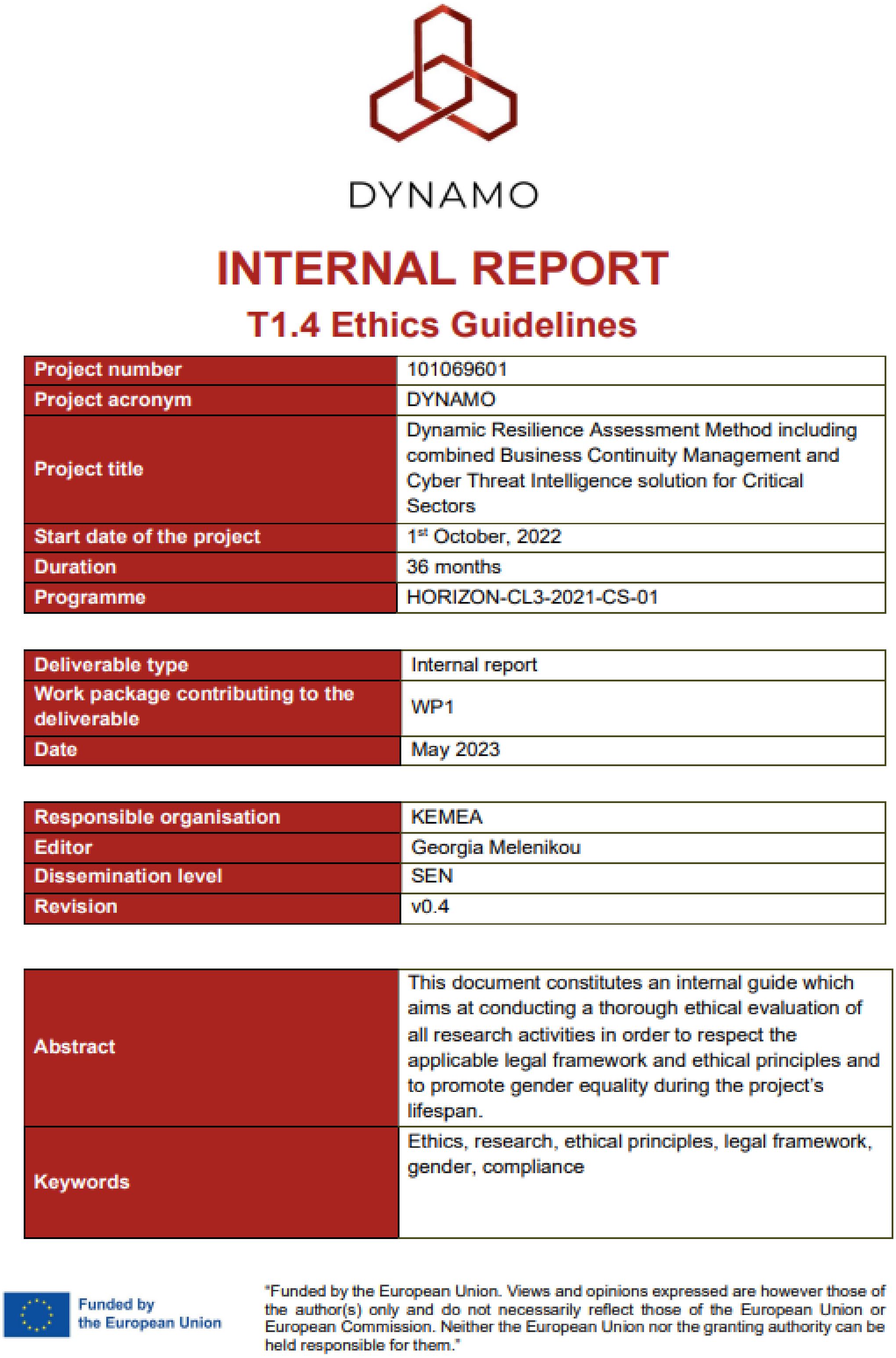
[11] European Parliament, P9_TA (2024)0138 Artificial Intelligence Act European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

[12] European Union Agency for Cybersecurity (ENISA), Multilayer Framework for Good Cybersecurity Practices for AI, June 2023

[13] Grant Agreement Project 101069601 - DYNAMO

[14] Regulation (EU) 2016/679 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)

Annex: Internal guide (Ethics Guidelines)



DYNAMO

INTERNAL REPORT

T1.4 Ethics Guidelines

Project number	101069601
Project acronym	DYNAMO
Project title	Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors
Start date of the project	1st October, 2022
Duration	36 months
Programme	HORIZON-CL3-2021-CS-01

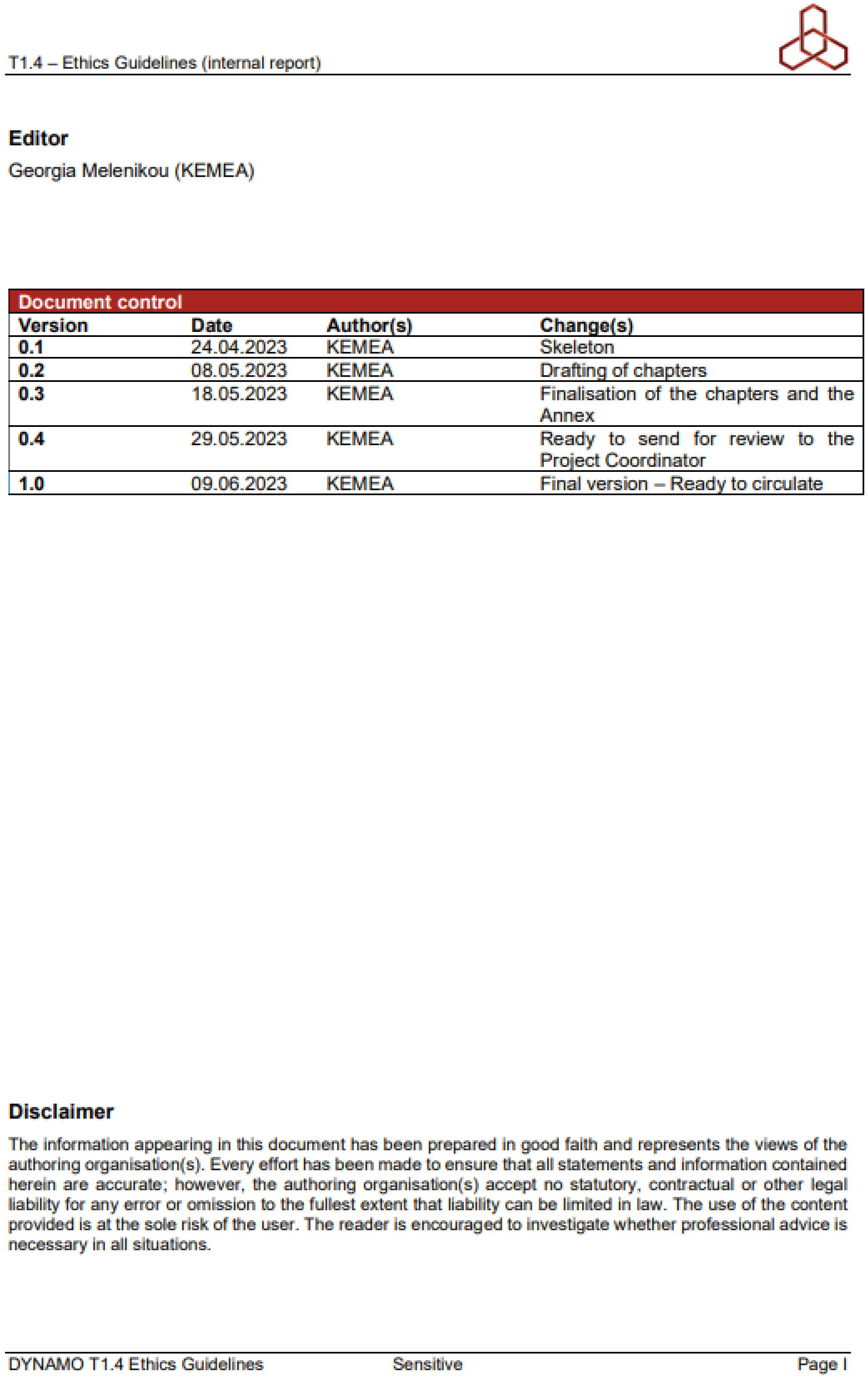
Deliverable type	Internal report
Work package contributing to the deliverable	WP1
Date	May 2023

Responsible organisation	KEMEA
Editor	Georgia Melenikou
Dissemination level	SEN
Revision	v0.4

Abstract	This document constitutes an internal guide which aims at conducting a thorough ethical evaluation of all research activities in order to respect the applicable legal framework and ethical principles and to promote gender equality during the project's lifespan.
Keywords	Ethics, research, ethical principles, legal framework, gender, compliance

Funded by the European Union

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them."



T1.4 – Ethics Guidelines (internal report)

Editor

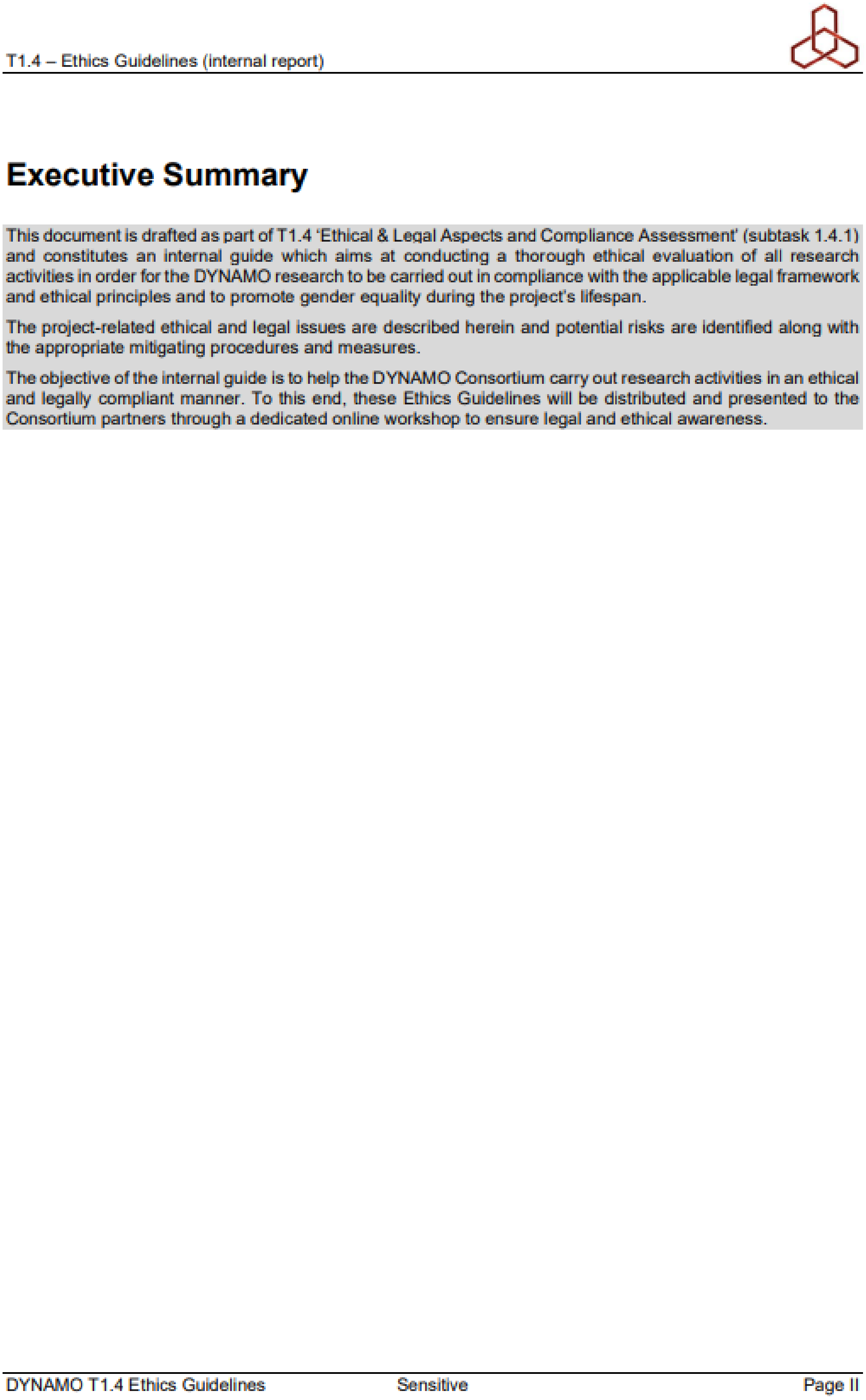
Georgia Melenikou (KEMEA)

Document control			
Version	**Date**	**Author(s)**	**Change(s)**
0.1	24.04.2023	KEMEA	Skeleton
0.2	08.05.2023	KEMEA	Drafting of chapters
0.3	18.05.2023	KEMEA	Finalisation of the chapters and the Annex
0.4	29.05.2023	KEMEA	Ready to send for review to the Project Coordinator
1.0	09.06.2023	KEMEA	Final version – Ready to circulate

Disclaimer

The information appearing in this document has been prepared in good faith and represents the views of the authoring organisation(s). Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authoring organisation(s) accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

DYNAMO T1.4 Ethics Guidelines Sensitive Page I

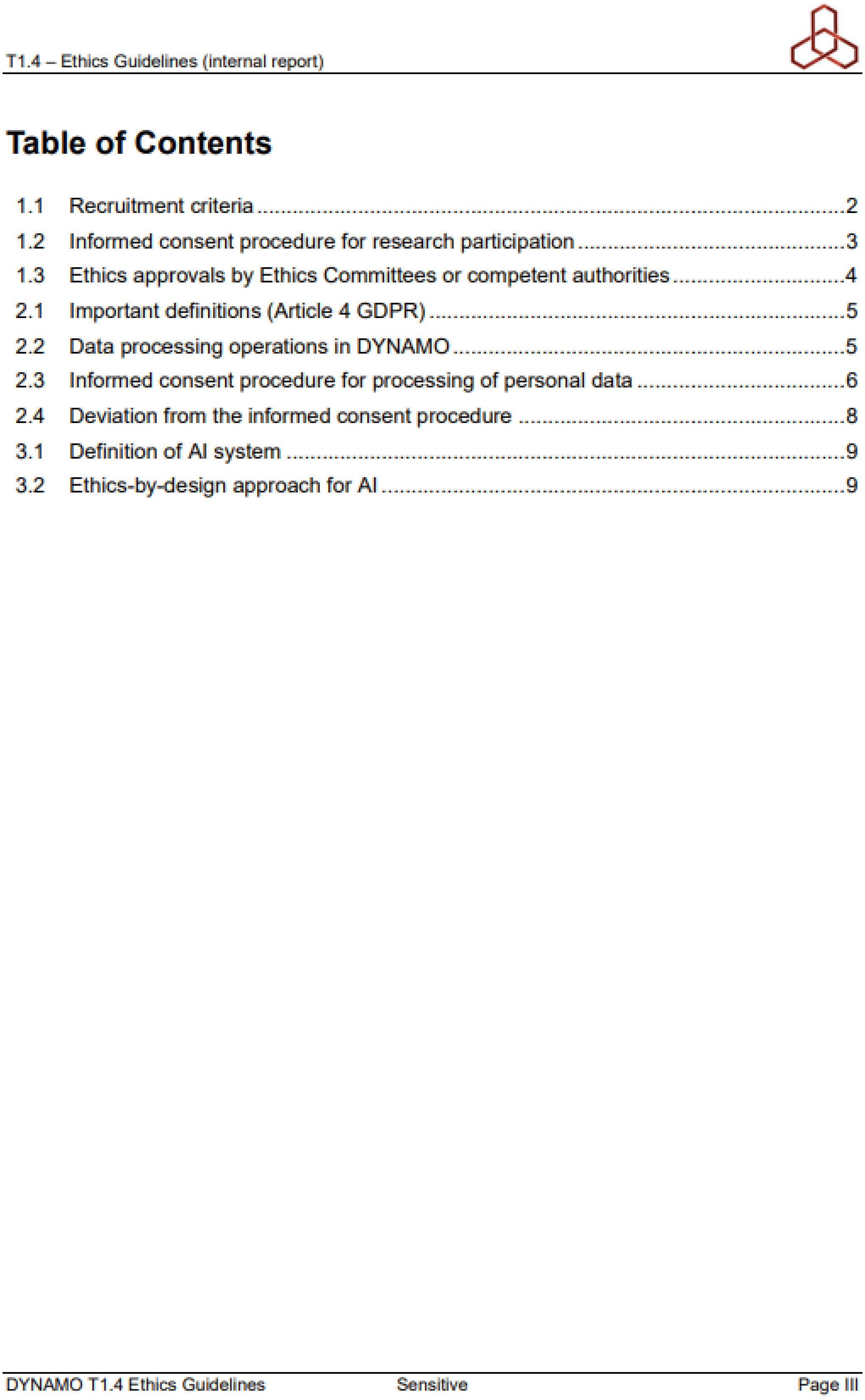


Executive Summary

This document is drafted as part of T1.4 'Ethical & Legal Aspects and Compliance Assessment' (subtask 1.4.1) and constitutes an internal guide which aims at conducting a thorough ethical evaluation of all research activities in order for the DYNAMO research to be carried out in compliance with the applicable legal framework and ethical principles and to promote gender equality during the project's lifespan.

The project-related ethical and legal issues are described herein and potential risks are identified along with the appropriate mitigating procedures and measures.

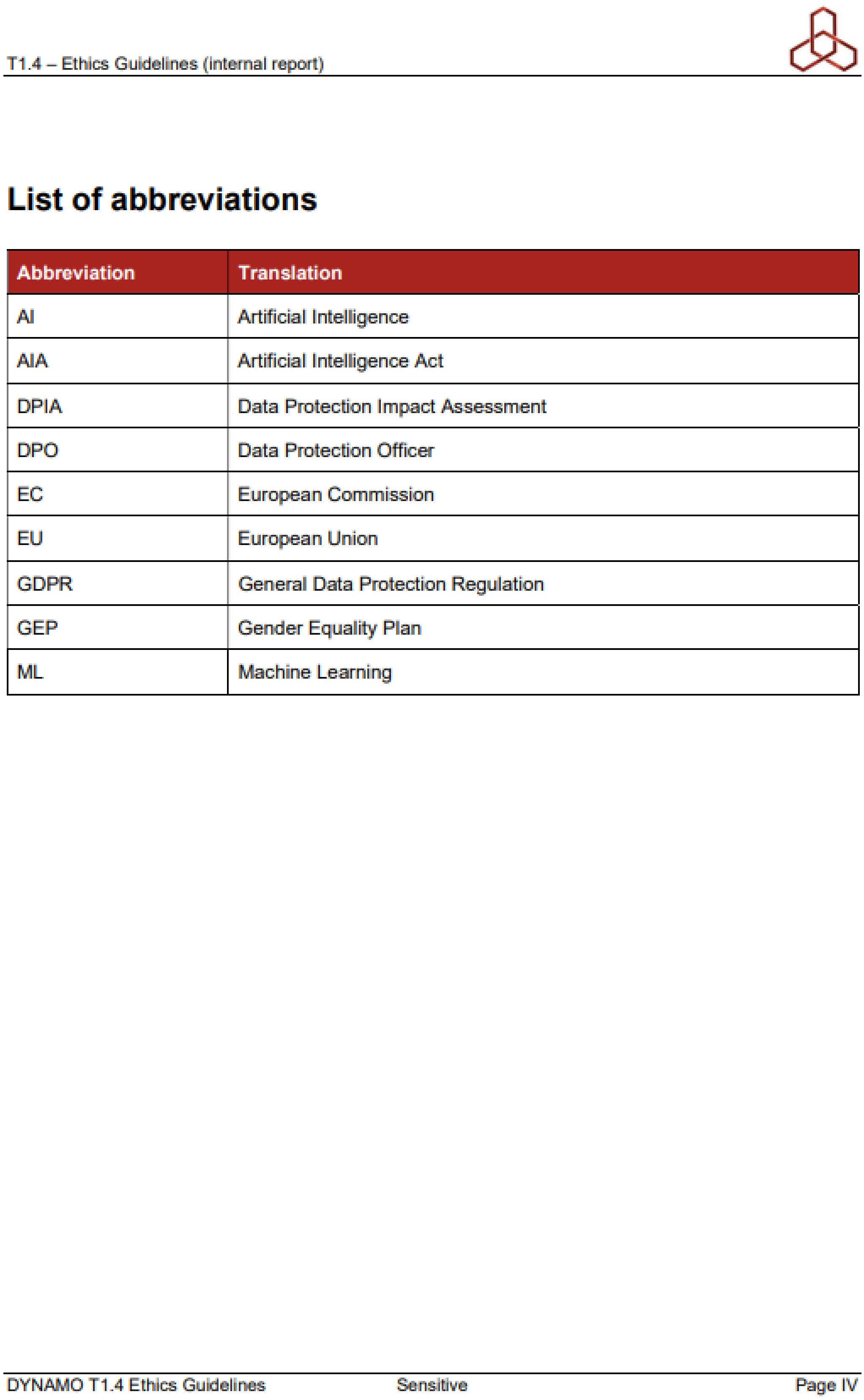
The objective of the internal guide is to help the DYNAMO Consortium carry out research activities in an ethical and legally compliant manner. To this end, these Ethics Guidelines will be distributed and presented to the Consortium partners through a dedicated online workshop to ensure legal and ethical awareness.



T1.4 – Ethics Guidelines (internal report)

Table of Contents

DYNAMO T1.4 Ethics Guidelines Sensitive Page III

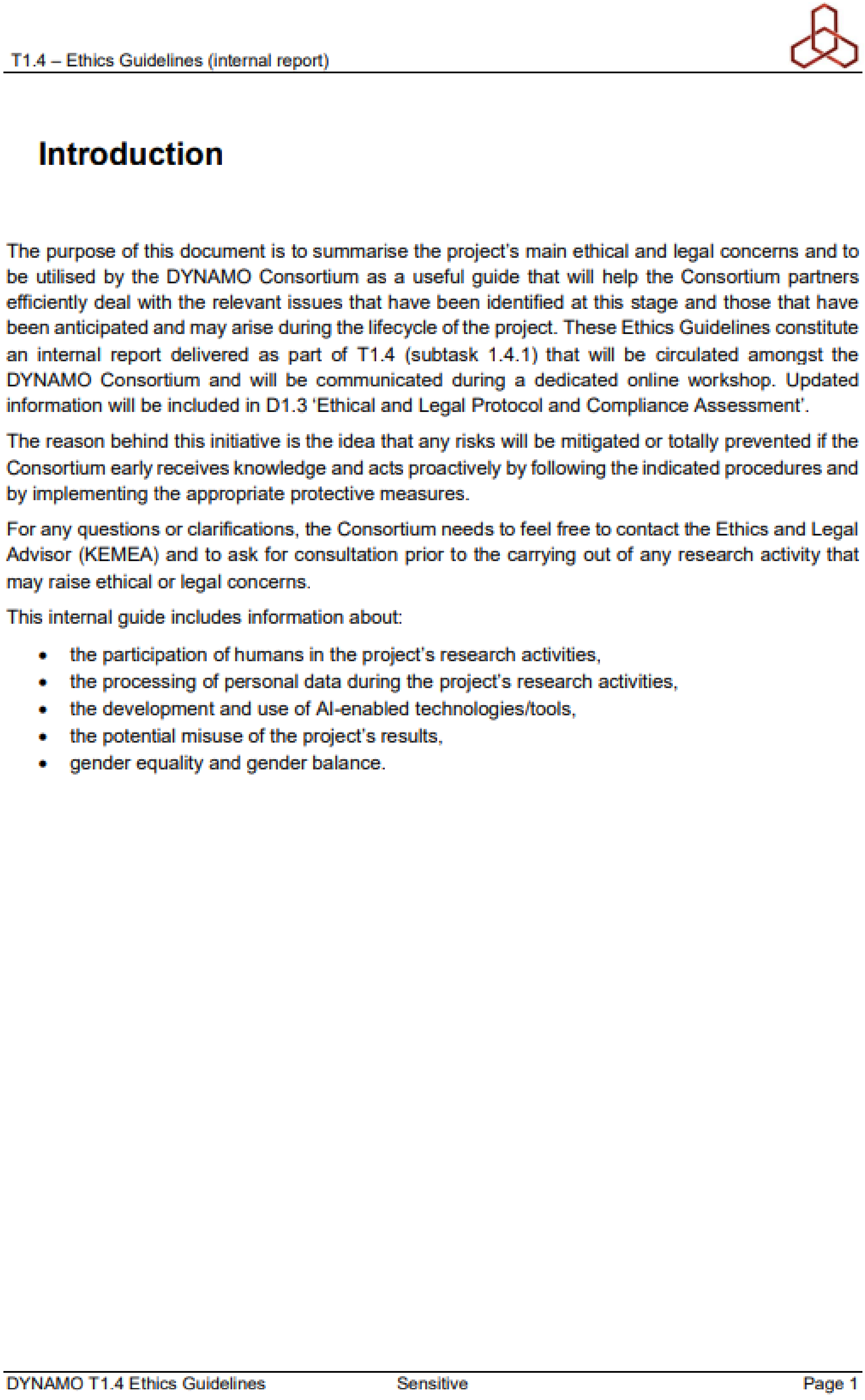


T1.4 – Ethics Guidelines (internal report)

List of abbreviations

Abbreviation	Translation
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
GEP	Gender Equality Plan
ML	Machine Learning

DYNAMO T1.4 Ethics Guidelines Sensitive Page IV



T1.4 – Ethics Guidelines (internal report)

Introduction

The purpose of this document is to summarise the project's main ethical and legal concerns and to be utilised by the DYNAMO Consortium as a useful guide that will help the Consortium partners efficiently deal with the relevant issues that have been identified at this stage and those that have been anticipated and may arise during the lifecycle of the project. These Ethics Guidelines constitute an internal report delivered as part of T1.4 (subtask 1.4.1) that will be circulated amongst the DYNAMO Consortium and will be communicated during a dedicated online workshop. Updated information will be included in D1.3 'Ethical and Legal Protocol and Compliance Assessment'.

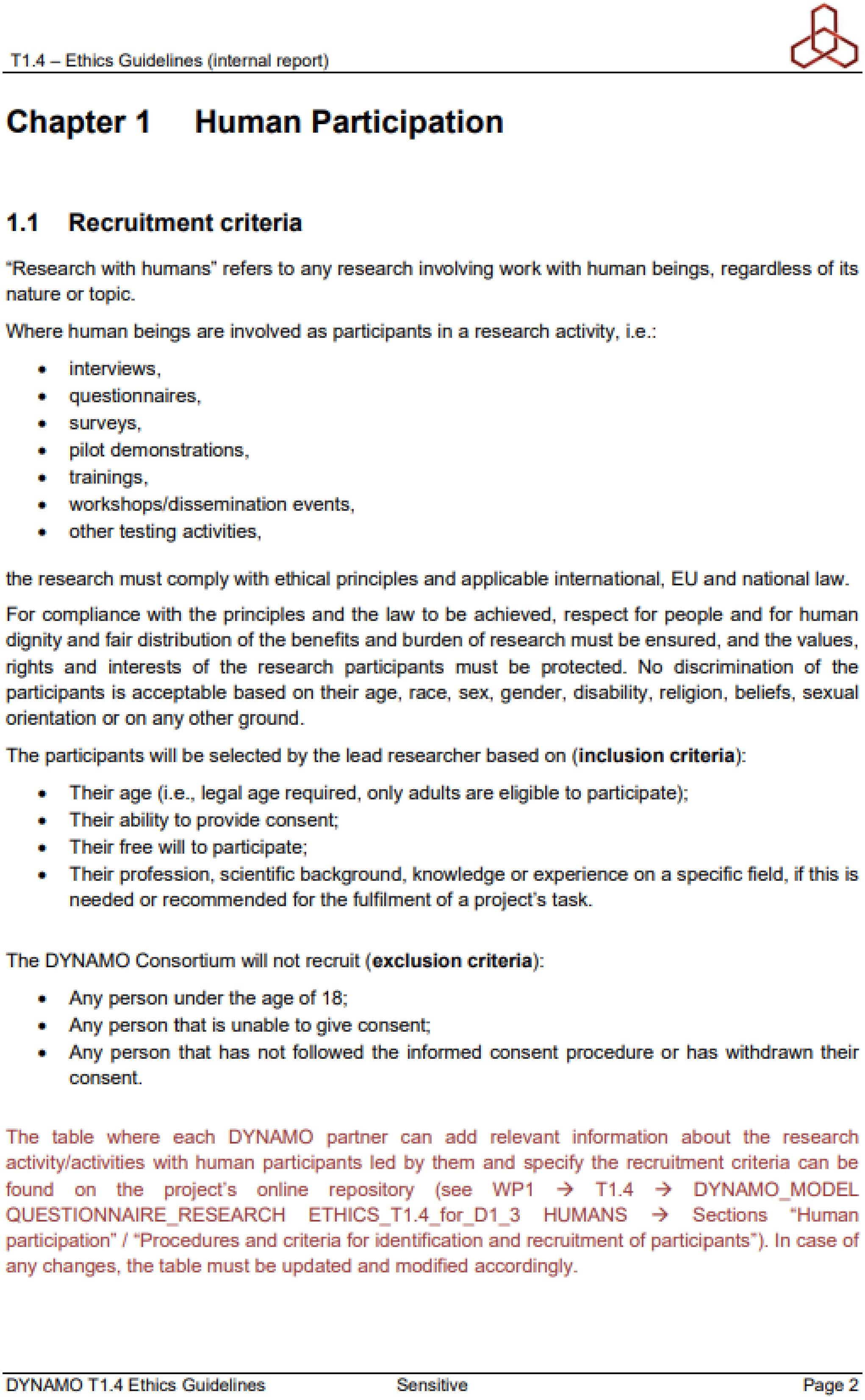
The reason behind this initiative is the idea that any risks will be mitigated or totally prevented if the Consortium early receives knowledge and acts proactively by following the indicated procedures and by implementing the appropriate protective measures.

For any questions or clarifications, the Consortium needs to feel free to contact the Ethics and Legal Advisor (KEMEA) and to ask for consultation prior to the carrying out of any research activity that may raise ethical or legal concerns.

This internal guide includes information about:

- the participation of humans in the project's research activities,
- the processing of personal data during the project's research activities,
- the development and use of AI-enabled technologies/tools,
- the potential misuse of the project's results,
- gender equality and gender balance.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 1



T1.4 – Ethics Guidelines (internal report)

Chapter 1 Human Participation

1.1 Recruitment criteria

“Research with humans” refers to any research involving work with human beings, regardless of its nature or topic.

Where human beings are involved as participants in a research activity, i.e.:

- interviews,
- questionnaires,
- surveys,
- pilot demonstrations,
- trainings,
- workshops/dissemination events,
- other testing activities,

the research must comply with ethical principles and applicable international, EU and national law.

For compliance with the principles and the law to be achieved, respect for people and for human dignity and fair distribution of the benefits and burden of research must be ensured, and the values, rights and interests of the research participants must be protected. No discrimination of the participants is acceptable based on their age, race, sex, gender, disability, religion, beliefs, sexual orientation or on any other ground.

The participants will be selected by the lead researcher based on (**inclusion criteria**):

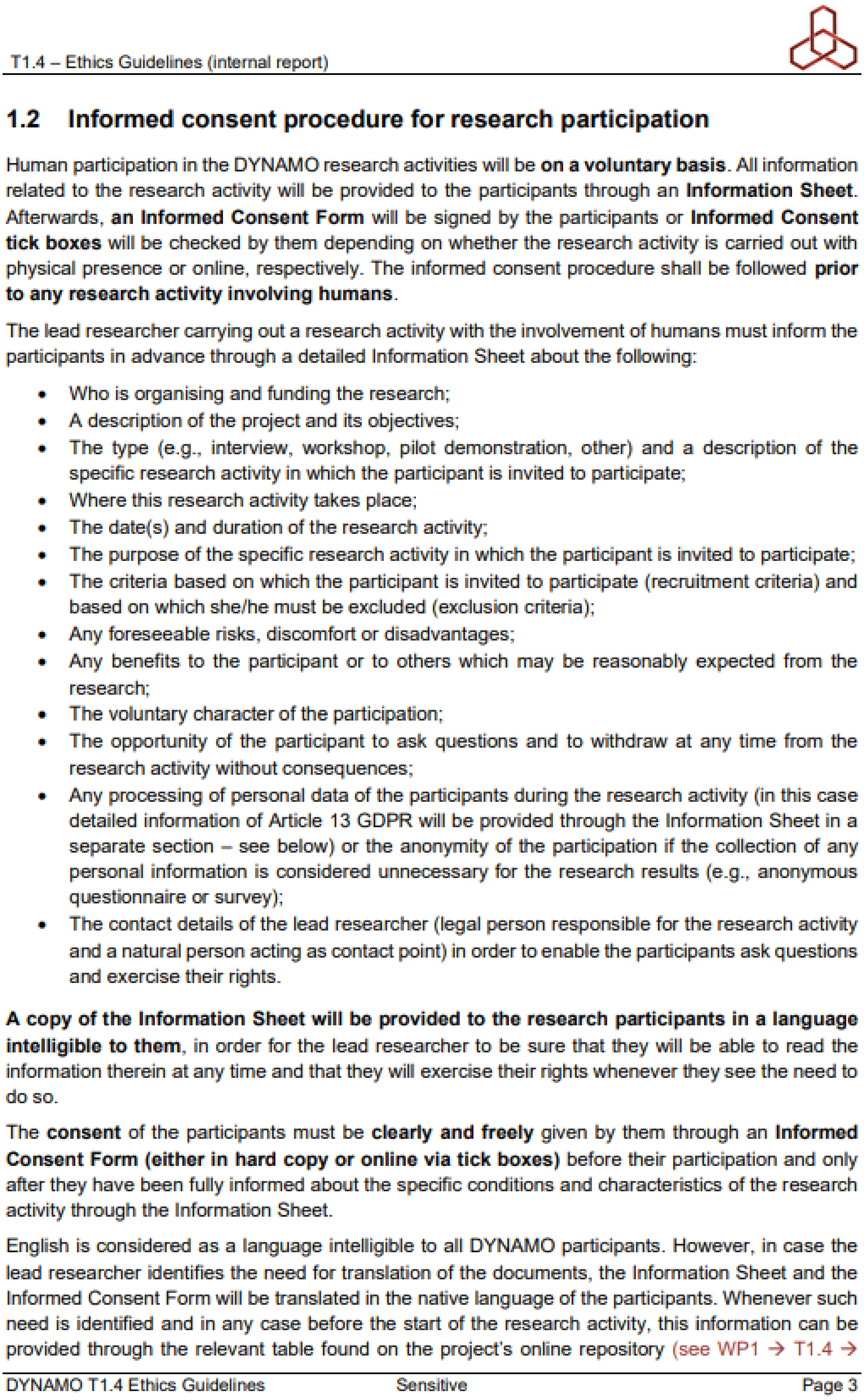
- Their age (i.e., legal age required, only adults are eligible to participate);
- Their ability to provide consent;
- Their free will to participate;
- Their profession, scientific background, knowledge or experience on a specific field, if this is needed or recommended for the fulfilment of a project’s task.

The DYNAMO Consortium will not recruit (**exclusion criteria**):

- Any person under the age of 18;
- Any person that is unable to give consent;
- Any person that has not followed the informed consent procedure or has withdrawn their consent.

The table where each DYNAMO partner can add relevant information about the research activity/activities with human participants led by them and specify the recruitment criteria can be found on the project’s online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 HUMANS → Sections “Human participation” / “Procedures and criteria for identification and recruitment of participants”). In case of any changes, the table must be updated and modified accordingly.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 2



1.2 Informed consent procedure for research participation

Human participation in the DYNAMO research activities will be **on a voluntary basis**. All information related to the research activity will be provided to the participants through an **Information Sheet**. Afterwards, **an Informed Consent Form** will be signed by the participants or **Informed Consent tick boxes** will be checked by them depending on whether the research activity is carried out with physical presence or online, respectively. The informed consent procedure shall be followed **prior to any research activity involving humans**.

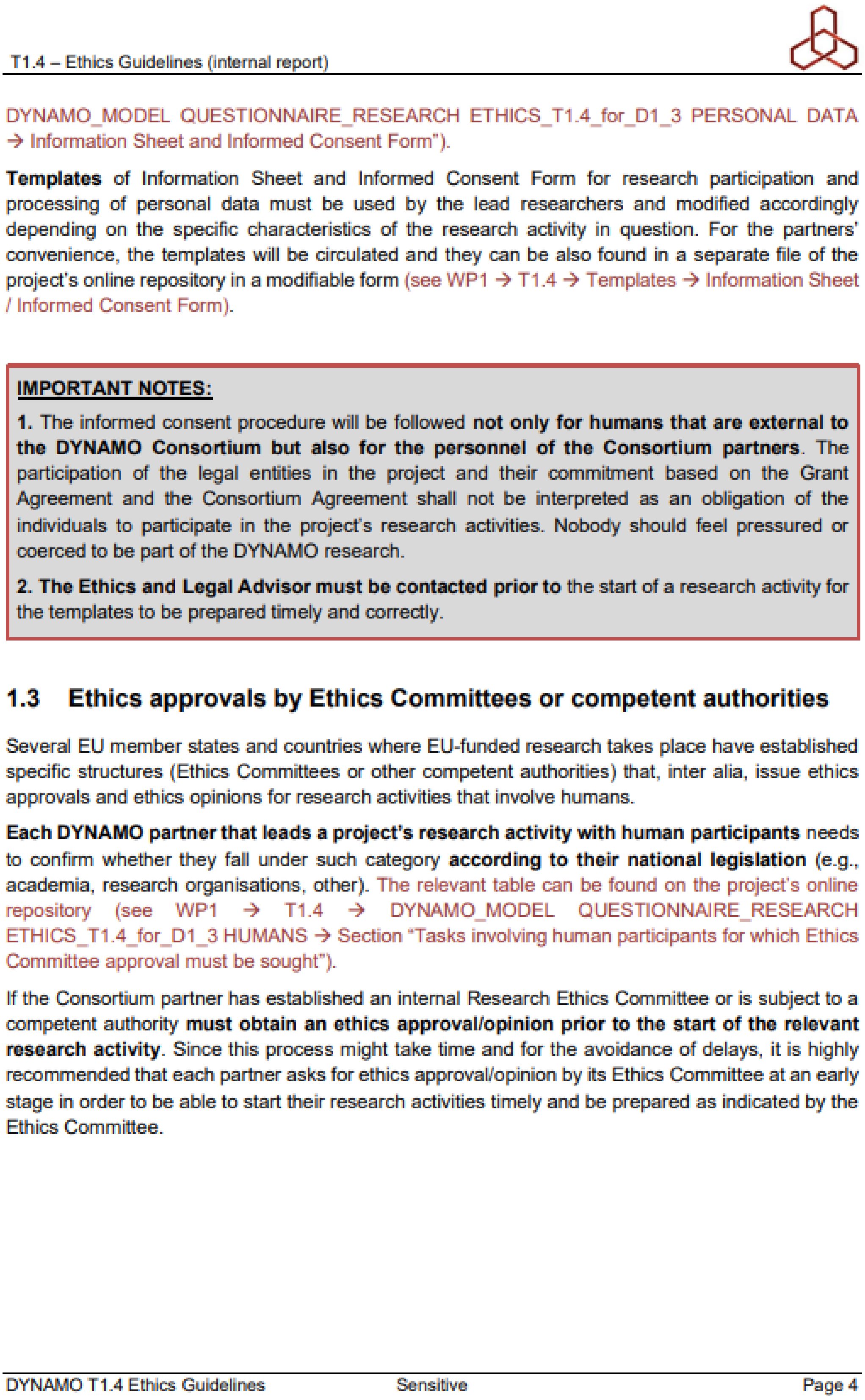
The lead researcher carrying out a research activity with the involvement of humans must inform the participants in advance through a detailed Information Sheet about the following:

- Who is organising and funding the research;
- A description of the project and its objectives;
- The type (e.g., interview, workshop, pilot demonstration, other) and a description of the specific research activity in which the participant is invited to participate;
- Where this research activity takes place;
- The date(s) and duration of the research activity;
- The purpose of the specific research activity in which the participant is invited to participate;
- The criteria based on which the participant is invited to participate (recruitment criteria) and based on which she/he must be excluded (exclusion criteria);
- Any foreseeable risks, discomfort or disadvantages;
- Any benefits to the participant or to others which may be reasonably expected from the research;
- The voluntary character of the participation;
- The opportunity of the participant to ask questions and to withdraw at any time from the research activity without consequences;
- Any processing of personal data of the participants during the research activity (in this case detailed information of Article 13 GDPR will be provided through the Information Sheet in a separate section – see below) or the anonymity of the participation if the collection of any personal information is considered unnecessary for the research results (e.g., anonymous questionnaire or survey);
- The contact details of the lead researcher (legal person responsible for the research activity and a natural person acting as contact point) in order to enable the participants ask questions and exercise their rights.

A copy of the Information Sheet will be provided to the research participants in a language intelligible to them, in order for the lead researcher to be sure that they will be able to read the information therein at any time and that they will exercise their rights whenever they see the need to do so.

The **consent** of the participants must be **clearly and freely** given by them through an **Informed Consent Form (either in hard copy or online via tick boxes)** before their participation and only after they have been fully informed about the specific conditions and characteristics of the research activity through the Information Sheet.

English is considered as a language intelligible to all DYNAMO participants. However, in case the lead researcher identifies the need for translation of the documents, the Information Sheet and the Informed Consent Form will be translated in the native language of the participants. Whenever such need is identified and in any case before the start of the research activity, this information can be provided through the relevant table found on the project's online repository (see WP1 → T1.4 →



T1.4 – Ethics Guidelines (internal report)

DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 PERSONAL DATA → Information Sheet and Informed Consent Form").

Templates of Information Sheet and Informed Consent Form for research participation and processing of personal data must be used by the lead researchers and modified accordingly depending on the specific characteristics of the research activity in question. For the partners' convenience, the templates will be circulated and they can be also found in a separate file of the project's online repository in a modifiable form (see WP1 → T1.4 → Templates → Information Sheet / Informed Consent Form).

IMPORTANT NOTES:

1. The informed consent procedure will be followed **not only for humans that are external to the DYNAMO Consortium but also for the personnel of the Consortium partners**. The participation of the legal entities in the project and their commitment based on the Grant Agreement and the Consortium Agreement shall not be interpreted as an obligation of the individuals to participate in the project's research activities. Nobody should feel pressured or coerced to be part of the DYNAMO research.

2. The Ethics and Legal Advisor must be contacted prior to the start of a research activity for the templates to be prepared timely and correctly.

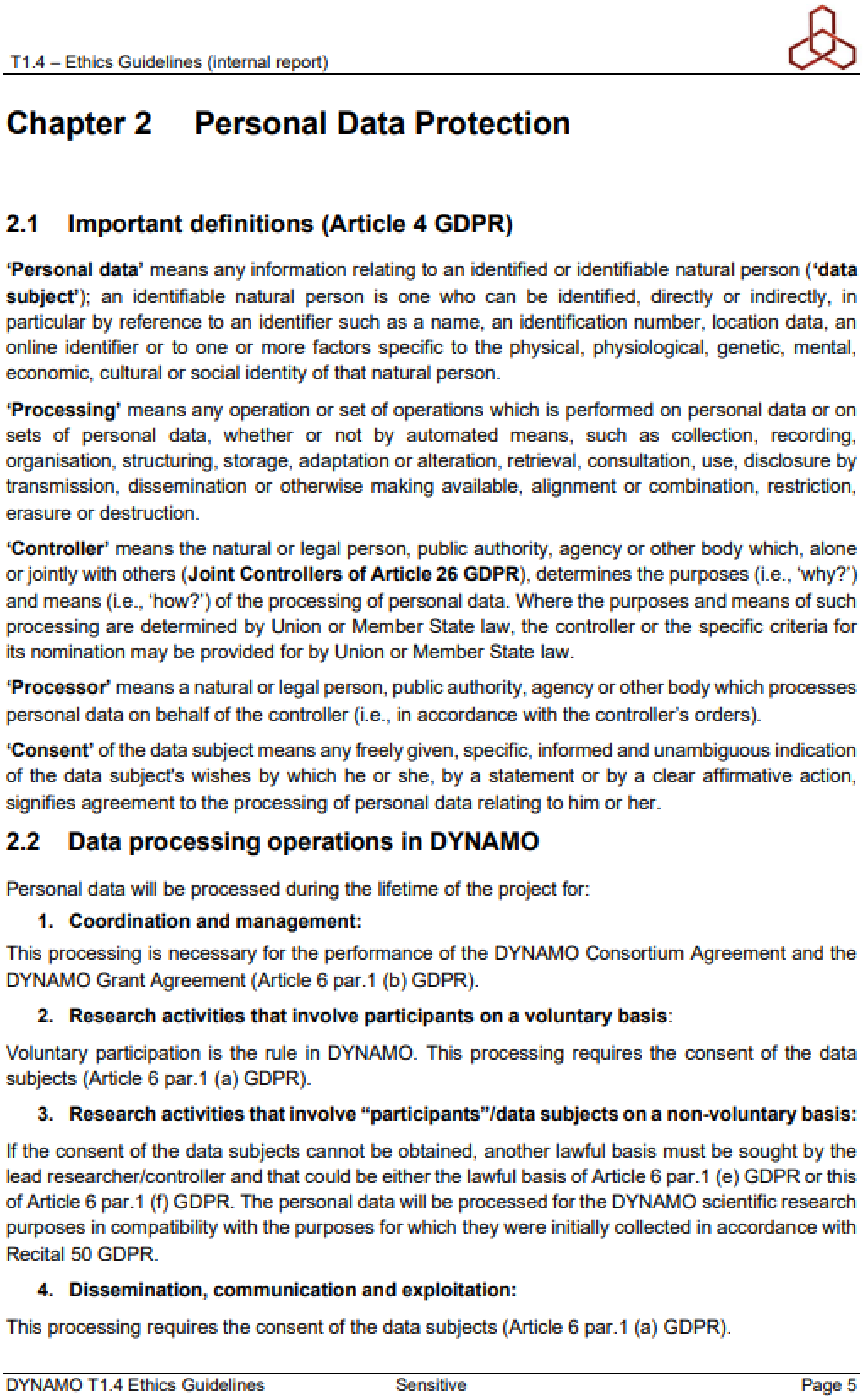
1.3 Ethics approvals by Ethics Committees or competent authorities

Several EU member states and countries where EU-funded research takes place have established specific structures (Ethics Committees or other competent authorities) that, inter alia, issue ethics approvals and ethics opinions for research activities that involve humans.

Each DYNAMO partner that leads a project's research activity with human participants needs to confirm whether they fall under such category **according to their national legislation** (e.g., academia, research organisations, other). The relevant table can be found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 HUMANS → Section "Tasks involving human participants for which Ethics Committee approval must be sought").

If the Consortium partner has established an internal Research Ethics Committee or is subject to a competent authority **must obtain an ethics approval/opinion prior to the start of the relevant research activity**. Since this process might take time and for the avoidance of delays, it is highly recommended that each partner asks for ethics approval/opinion by its Ethics Committee at an early stage in order to be able to start their research activities timely and be prepared as indicated by the Ethics Committee.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 4



T1.4 – Ethics Guidelines (internal report)

Chapter 2 Personal Data Protection

2.1 Important definitions (Article 4 GDPR)

'Personal data' means any information relating to an identified or identifiable natural person (**'data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others (**Joint Controllers of Article 26 GDPR**), determines the purposes (i.e., 'why?') and means (i.e., 'how?') of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (i.e., in accordance with the controller's orders).

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

2.2 Data processing operations in DYNAMO

Personal data will be processed during the lifetime of the project for:

1. **Coordination and management:**

This processing is necessary for the performance of the DYNAMO Consortium Agreement and the DYNAMO Grant Agreement (Article 6 par.1 (b) GDPR).

2. **Research activities that involve participants on a voluntary basis**:

Voluntary participation is the rule in DYNAMO. This processing requires the consent of the data subjects (Article 6 par.1 (a) GDPR).

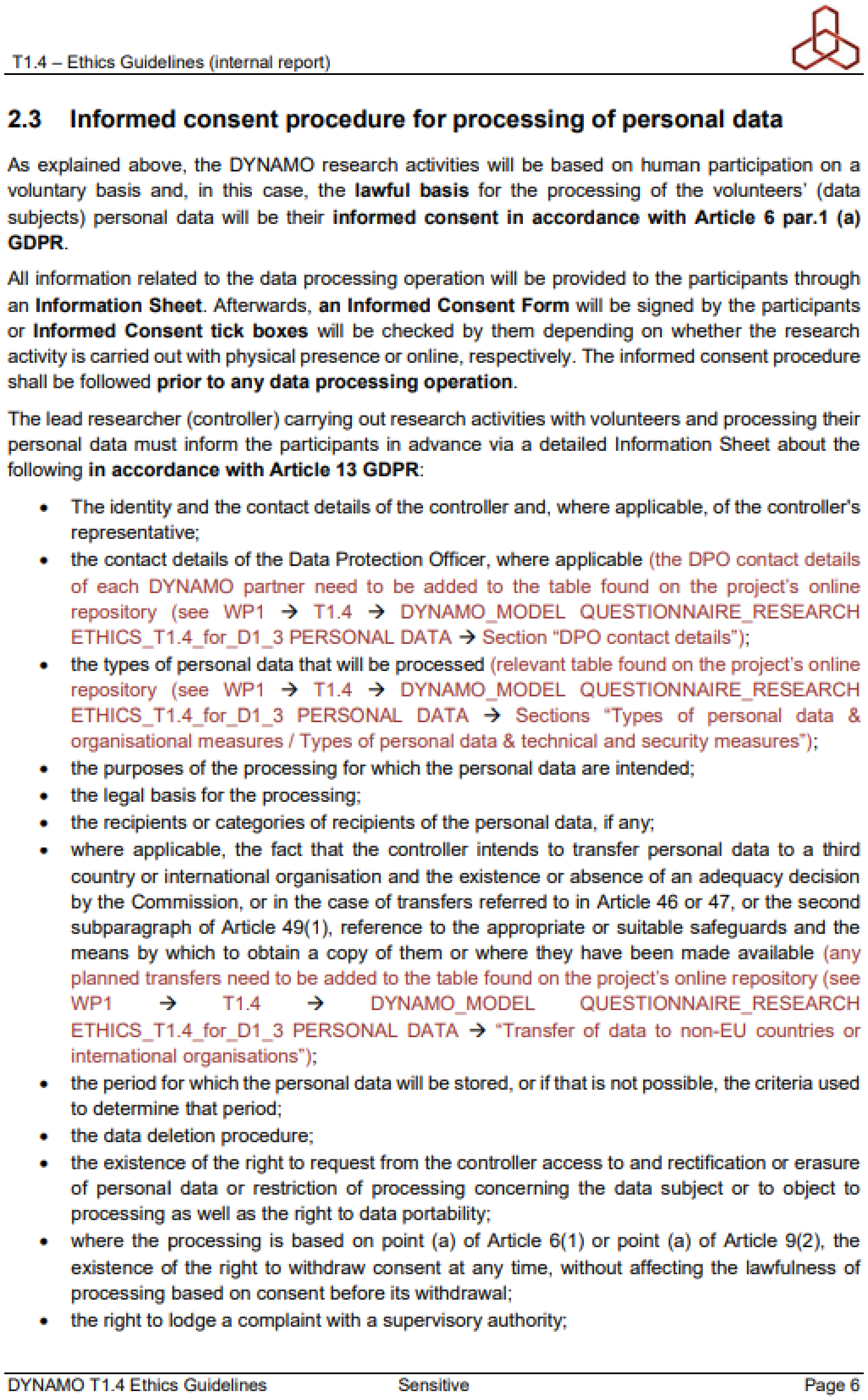
3. **Research activities that involve "participants"/data subjects on a non-voluntary basis:**

If the consent of the data subjects cannot be obtained, another lawful basis must be sought by the lead researcher/controller and that could be either the lawful basis of Article 6 par.1 (e) GDPR or this of Article 6 par.1 (f) GDPR. The personal data will be processed for the DYNAMO scientific research purposes in compatibility with the purposes for which they were initially collected in accordance with Recital 50 GDPR.

4. **Dissemination, communication and exploitation:**

This processing requires the consent of the data subjects (Article 6 par.1 (a) GDPR).

DYNAMO T1.4 Ethics Guidelines Sensitive Page 5



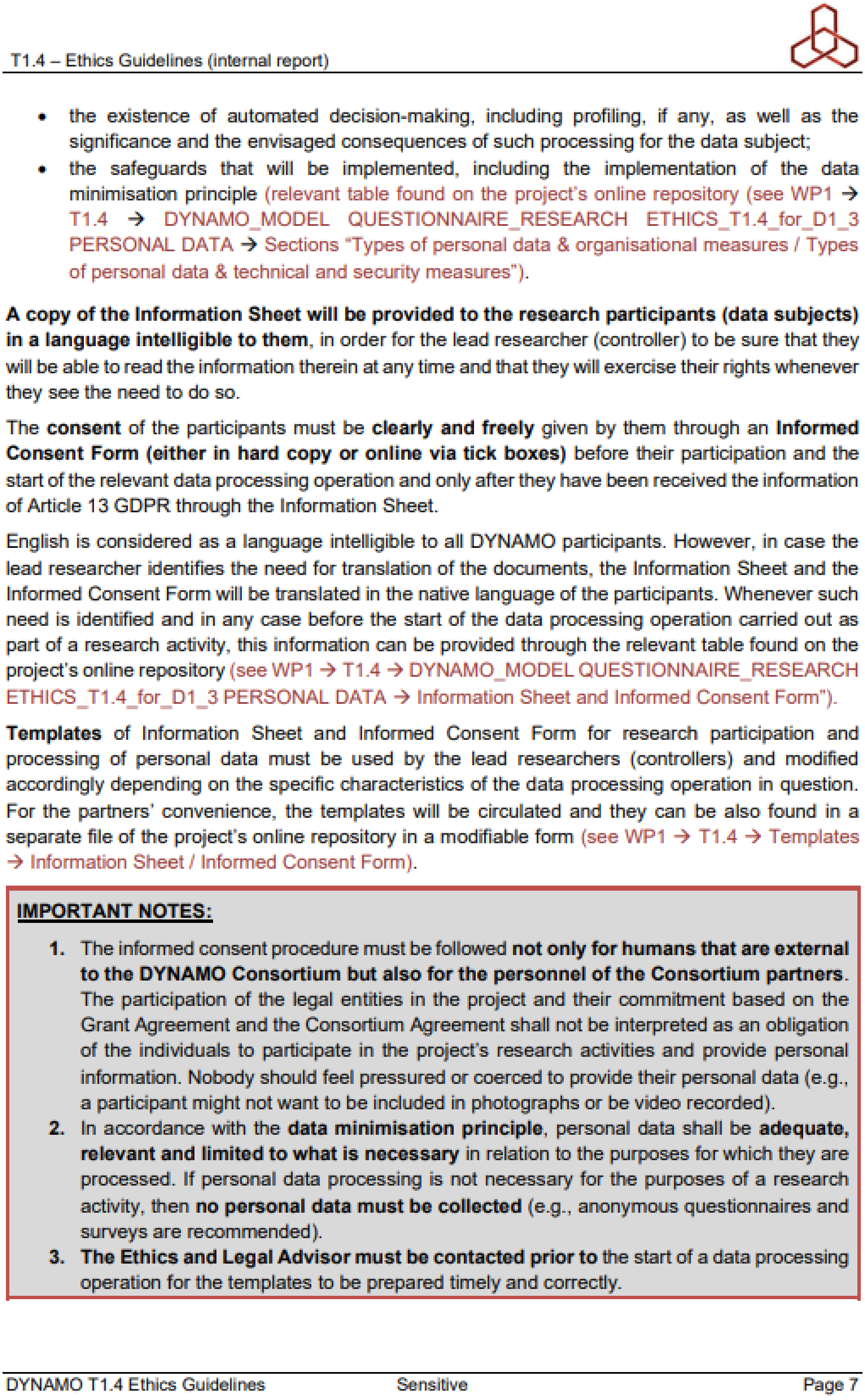
2.3 Informed consent procedure for processing of personal data

As explained above, the DYNAMO research activities will be based on human participation on a voluntary basis and, in this case, the **lawful basis** for the processing of the volunteers' (data subjects) personal data will be their **informed consent in accordance with Article 6 par.1 (a) GDPR**.

All information related to the data processing operation will be provided to the participants through an **Information Sheet**. Afterwards, **an Informed Consent Form** will be signed by the participants or **Informed Consent tick boxes** will be checked by them depending on whether the research activity is carried out with physical presence or online, respectively. The informed consent procedure shall be followed **prior to any data processing operation**.

The lead researcher (controller) carrying out research activities with volunteers and processing their personal data must inform the participants in advance via a detailed Information Sheet about the following **in accordance with Article 13 GDPR**:

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the Data Protection Officer, where applicable (the DPO contact details of each DYNAMO partner need to be added to the table found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 PERSONAL DATA → Section "DPO contact details");
- the types of personal data that will be processed (relevant table found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 PERSONAL DATA → Sections "Types of personal data & organisational measures / Types of personal data & technical and security measures");
- the purposes of the processing for which the personal data are intended;
- the legal basis for the processing;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (any planned transfers need to be added to the table found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 PERSONAL DATA → "Transfer of data to non-EU countries or international organisations");
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the data deletion procedure;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;



T1.4 – Ethics Guidelines (internal report)

- the existence of automated decision-making, including profiling, if any, as well as the significance and the envisaged consequences of such processing for the data subject;
- the safeguards that will be implemented, including the implementation of the data minimisation principle (relevant table found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 PERSONAL DATA → Sections "Types of personal data & organisational measures / Types of personal data & technical and security measures").

A copy of the Information Sheet will be provided to the research participants (data subjects) in a language intelligible to them, in order for the lead researcher (controller) to be sure that they will be able to read the information therein at any time and that they will exercise their rights whenever they see the need to do so.

The **consent** of the participants must be **clearly and freely** given by them through an **Informed Consent Form (either in hard copy or online via tick boxes)** before their participation and the start of the relevant data processing operation and only after they have been received the information of Article 13 GDPR through the Information Sheet.

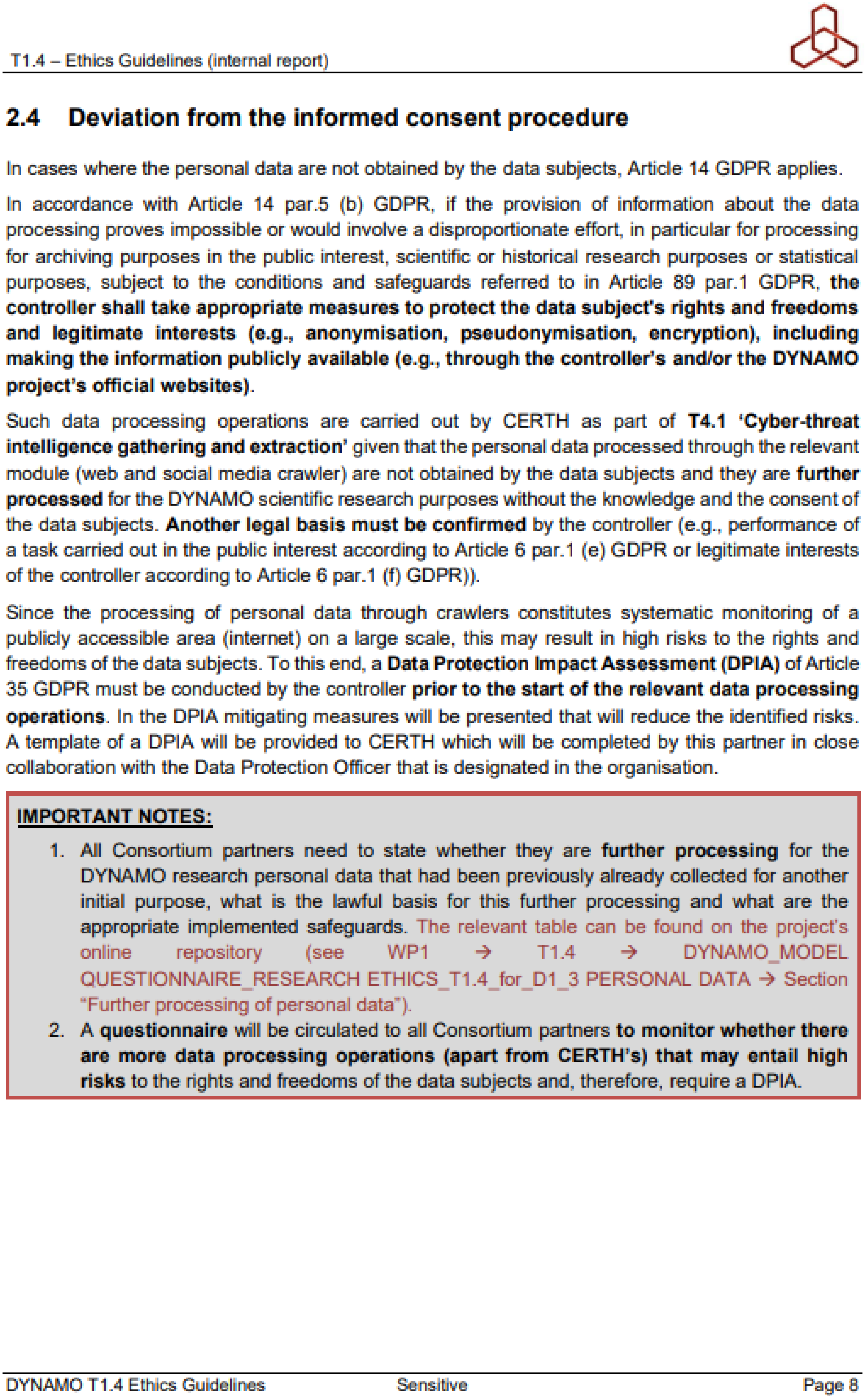
English is considered as a language intelligible to all DYNAMO participants. However, in case the lead researcher identifies the need for translation of the documents, the Information Sheet and the Informed Consent Form will be translated in the native language of the participants. Whenever such need is identified and in any case before the start of the data processing operation carried out as part of a research activity, this information can be provided through the relevant table found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 PERSONAL DATA → Information Sheet and Informed Consent Form").

Templates of Information Sheet and Informed Consent Form for research participation and processing of personal data must be used by the lead researchers (controllers) and modified accordingly depending on the specific characteristics of the data processing operation in question. For the partners' convenience, the templates will be circulated and they can be also found in a separate file of the project's online repository in a modifiable form (see WP1 → T1.4 → Templates → Information Sheet / Informed Consent Form).

IMPORTANT NOTES:

1. The informed consent procedure must be followed **not only for humans that are external to the DYNAMO Consortium but also for the personnel of the Consortium partners**. The participation of the legal entities in the project and their commitment based on the Grant Agreement and the Consortium Agreement shall not be interpreted as an obligation of the individuals to participate in the project's research activities and provide personal information. Nobody should feel pressured or coerced to provide their personal data (e.g., a participant might not want to be included in photographs or be video recorded).
2. In accordance with the **data minimisation principle**, personal data shall be **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed. If personal data processing is not necessary for the purposes of a research activity, then **no personal data must be collected** (e.g., anonymous questionnaires and surveys are recommended).
3. **The Ethics and Legal Advisor must be contacted prior to** the start of a data processing operation for the templates to be prepared timely and correctly.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 7



T1.4 – Ethics Guidelines (internal report)

2.4 Deviation from the informed consent procedure

In cases where the personal data are not obtained by the data subjects, Article 14 GDPR applies.

In accordance with Article 14 par.5 (b) GDPR, if the provision of information about the data processing proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89 par.1 GDPR, **the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests (e.g., anonymisation, pseudonymisation, encryption), including making the information publicly available (e.g., through the controller's and/or the DYNAMO project's official websites)**.

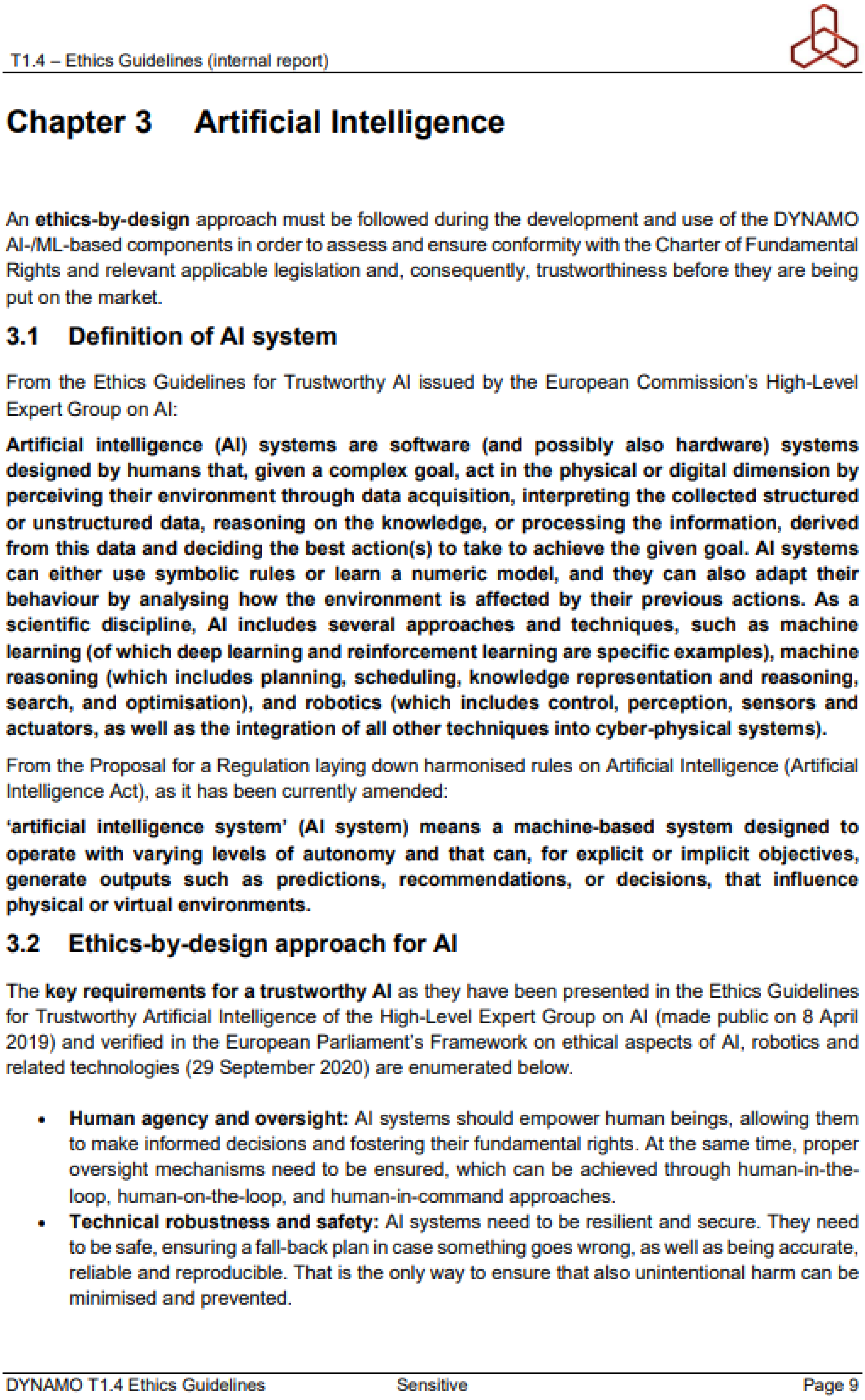
Such data processing operations are carried out by CERTH as part of **T4.1 'Cyber-threat intelligence gathering and extraction'** given that the personal data processed through the relevant module (web and social media crawler) are not obtained by the data subjects and they are **further processed** for the DYNAMO scientific research purposes without the knowledge and the consent of the data subjects. **Another legal basis must be confirmed** by the controller (e.g., performance of a task carried out in the public interest according to Article 6 par.1 (e) GDPR or legitimate interests of the controller according to Article 6 par.1 (f) GDPR)).

Since the processing of personal data through crawlers constitutes systematic monitoring of a publicly accessible area (internet) on a large scale, this may result in high risks to the rights and freedoms of the data subjects. To this end, a **Data Protection Impact Assessment (DPIA)** of Article 35 GDPR must be conducted by the controller **prior to the start of the relevant data processing operations**. In the DPIA mitigating measures will be presented that will reduce the identified risks. A template of a DPIA will be provided to CERTH which will be completed by this partner in close collaboration with the Data Protection Officer that is designated in the organisation.

IMPORTANT NOTES:

1. All Consortium partners need to state whether they are **further processing** for the DYNAMO research personal data that had been previously already collected for another initial purpose, what is the lawful basis for this further processing and what are the appropriate implemented safeguards. The relevant table can be found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 PERSONAL DATA → Section "Further processing of personal data").
2. A **questionnaire** will be circulated to all Consortium partners **to monitor whether there are more data processing operations (apart from CERTH's) that may entail high risks** to the rights and freedoms of the data subjects and, therefore, require a DPIA.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 8



T1.4 – Ethics Guidelines (internal report)

Chapter 3 Artificial Intelligence

An **ethics-by-design** approach must be followed during the development and use of the DYNAMO AI-/ML-based components in order to assess and ensure conformity with the Charter of Fundamental Rights and relevant applicable legislation and, consequently, trustworthiness before they are being put on the market.

3.1 Definition of AI system

From the Ethics Guidelines for Trustworthy AI issued by the European Commission's High-Level Expert Group on AI:

Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimisation), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).

From the Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act), as it has been currently amended:

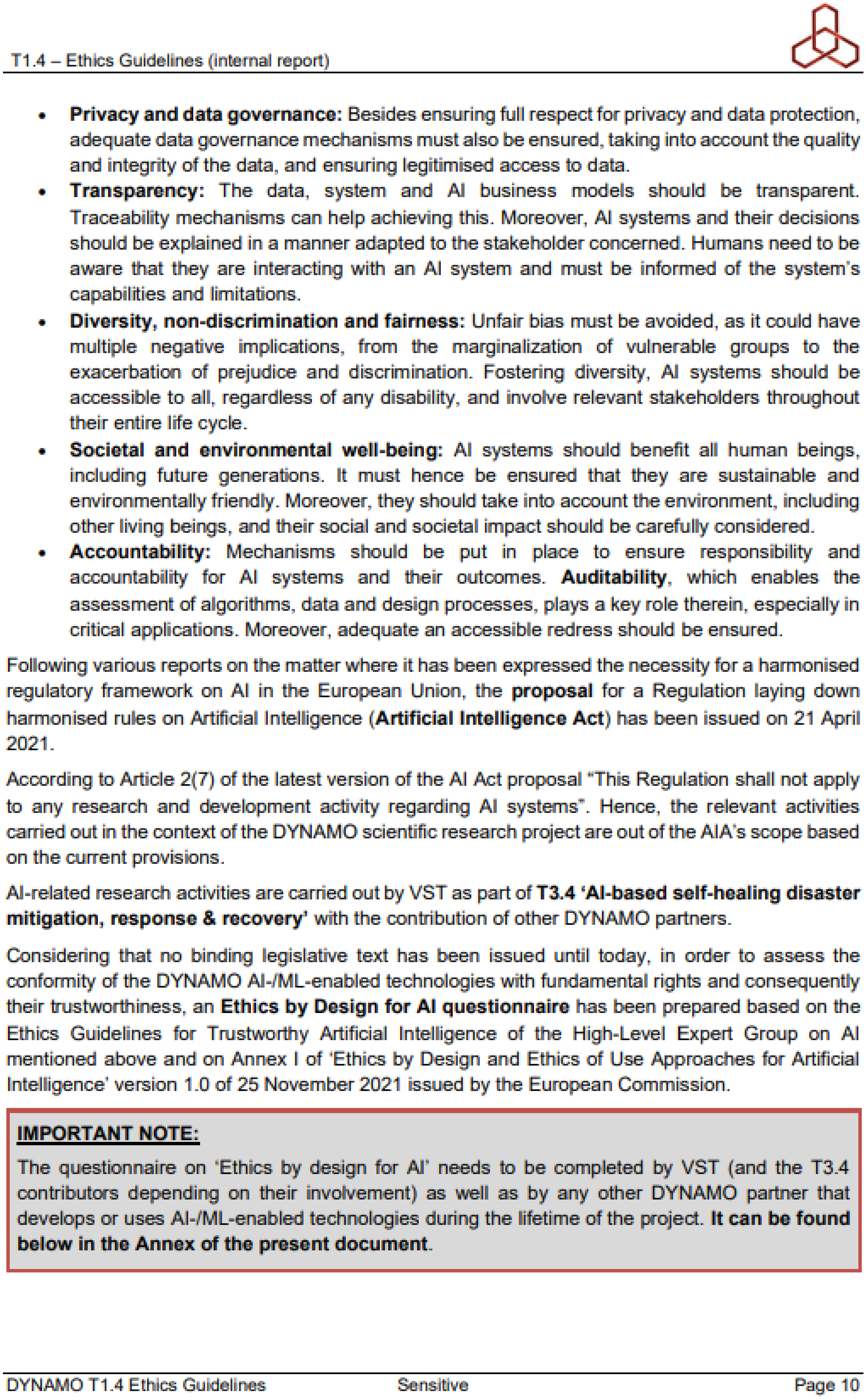
'artificial intelligence system' (AI system) means a machine-based system designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.

3.2 Ethics-by-design approach for AI

The **key requirements for a trustworthy AI** as they have been presented in the Ethics Guidelines for Trustworthy Artificial Intelligence of the High-Level Expert Group on AI (made public on 8 April 2019) and verified in the European Parliament's Framework on ethical aspects of AI, robotics and related technologies (29 September 2020) are enumerated below.

- **Human agency and oversight:** AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.
- **Technical robustness and safety:** AI systems need to be resilient and secure. They need to be safe, ensuring a fall-back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimised and prevented.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 9



T1.4 – Ethics Guidelines (internal report)

- **Privacy and data governance:** Besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimised access to data.
- **Transparency:** The data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system and must be informed of the system's capabilities and limitations.
- **Diversity, non-discrimination and fairness:** Unfair bias must be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life cycle.
- **Societal and environmental well-being:** AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered.
- **Accountability:** Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. **Auditability**, which enables the assessment of algorithms, data and design processes, plays a key role therein, especially in critical applications. Moreover, adequate an accessible redress should be ensured.

Following various reports on the matter where it has been expressed the necessity for a harmonised regulatory framework on AI in the European Union, the **proposal** for a Regulation laying down harmonised rules on Artificial Intelligence (**Artificial Intelligence Act**) has been issued on 21 April 2021.

According to Article 2(7) of the latest version of the AI Act proposal "This Regulation shall not apply to any research and development activity regarding AI systems". Hence, the relevant activities carried out in the context of the DYNAMO scientific research project are out of the AIA's scope based on the current provisions.

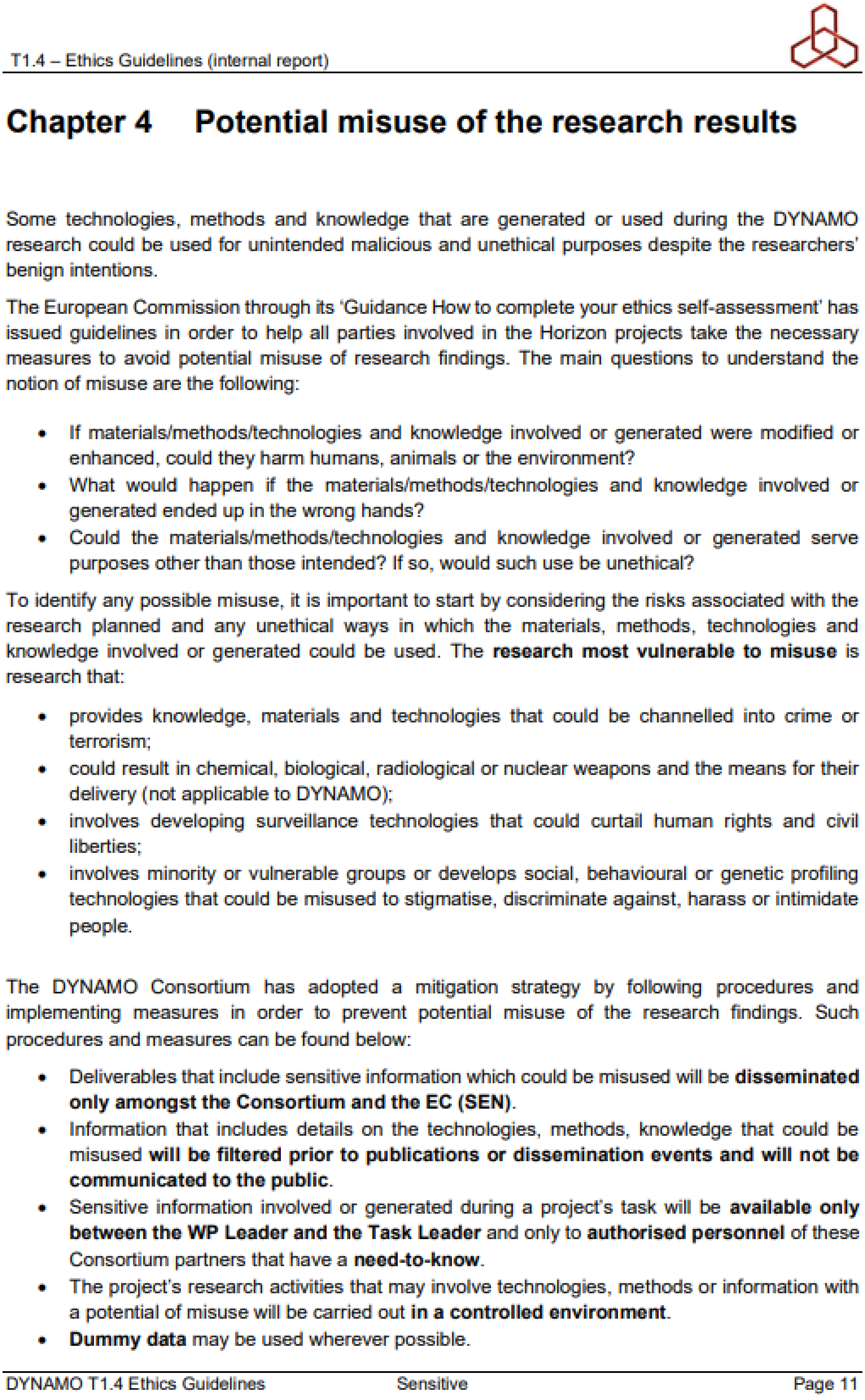
AI-related research activities are carried out by VST as part of **T3.4 'AI-based self-healing disaster mitigation, response & recovery'** with the contribution of other DYNAMO partners.

Considering that no binding legislative text has been issued until today, in order to assess the conformity of the DYNAMO AI-/ML-enabled technologies with fundamental rights and consequently their trustworthiness, an **Ethics by Design for AI questionnaire** has been prepared based on the Ethics Guidelines for Trustworthy Artificial Intelligence of the High-Level Expert Group on AI mentioned above and on Annex I of 'Ethics by Design and Ethics of Use Approaches for Artificial Intelligence' version 1.0 of 25 November 2021 issued by the European Commission.

IMPORTANT NOTE:

The questionnaire on 'Ethics by design for AI' needs to be completed by VST (and the T3.4 contributors depending on their involvement) as well as by any other DYNAMO partner that develops or uses AI-/ML-enabled technologies during the lifetime of the project. **It can be found below in the Annex of the present document**.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 10



T1.4 – Ethics Guidelines (internal report)

Chapter 4 Potential misuse of the research results

Some technologies, methods and knowledge that are generated or used during the DYNAMO research could be used for unintended malicious and unethical purposes despite the researchers' benign intentions.

The European Commission through its 'Guidance How to complete your ethics self-assessment' has issued guidelines in order to help all parties involved in the Horizon projects take the necessary measures to avoid potential misuse of research findings. The main questions to understand the notion of misuse are the following:

- If materials/methods/technologies and knowledge involved or generated were modified or enhanced, could they harm humans, animals or the environment?
- What would happen if the materials/methods/technologies and knowledge involved or generated ended up in the wrong hands?
- Could the materials/methods/technologies and knowledge involved or generated serve purposes other than those intended? If so, would such use be unethical?

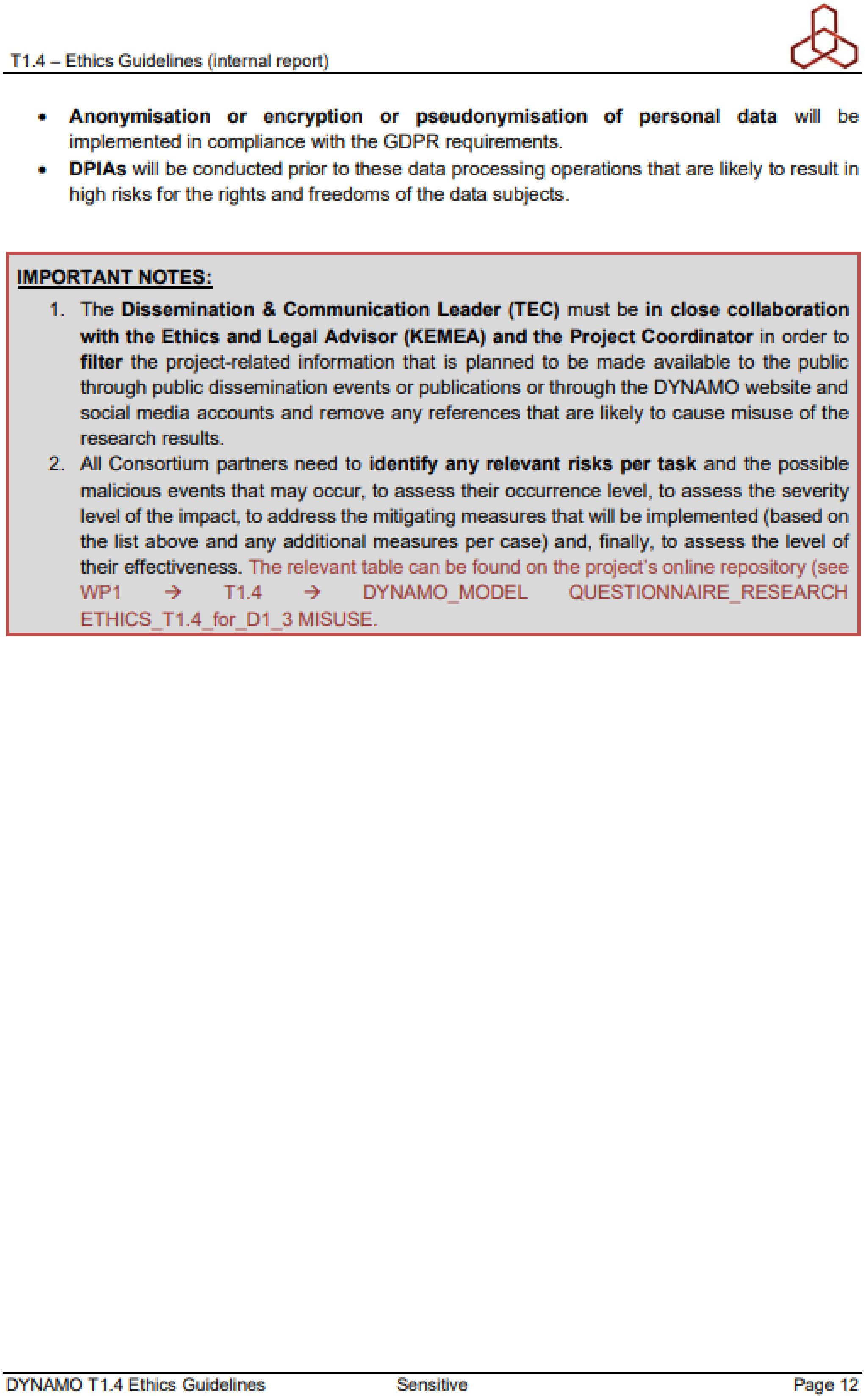
To identify any possible misuse, it is important to start by considering the risks associated with the research planned and any unethical ways in which the materials, methods, technologies and knowledge involved or generated could be used. The **research most vulnerable to misuse** is research that:

- provides knowledge, materials and technologies that could be channelled into crime or terrorism;
- could result in chemical, biological, radiological or nuclear weapons and the means for their delivery (not applicable to DYNAMO);
- involves developing surveillance technologies that could curtail human rights and civil liberties;
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

The DYNAMO Consortium has adopted a mitigation strategy by following procedures and implementing measures in order to prevent potential misuse of the research findings. Such procedures and measures can be found below:

- Deliverables that include sensitive information which could be misused will be **disseminated only amongst the Consortium and the EC (SEN)**.
- Information that includes details on the technologies, methods, knowledge that could be misused **will be filtered prior to publications or dissemination events and will not be communicated to the public**.
- Sensitive information involved or generated during a project's task will be **available only between the WP Leader and the Task Leader** and only to **authorised personnel** of these Consortium partners that have a **need-to-know**.
- The project's research activities that may involve technologies, methods or information with a potential of misuse will be carried out **in a controlled environment**.
- **Dummy data** may be used wherever possible.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 11



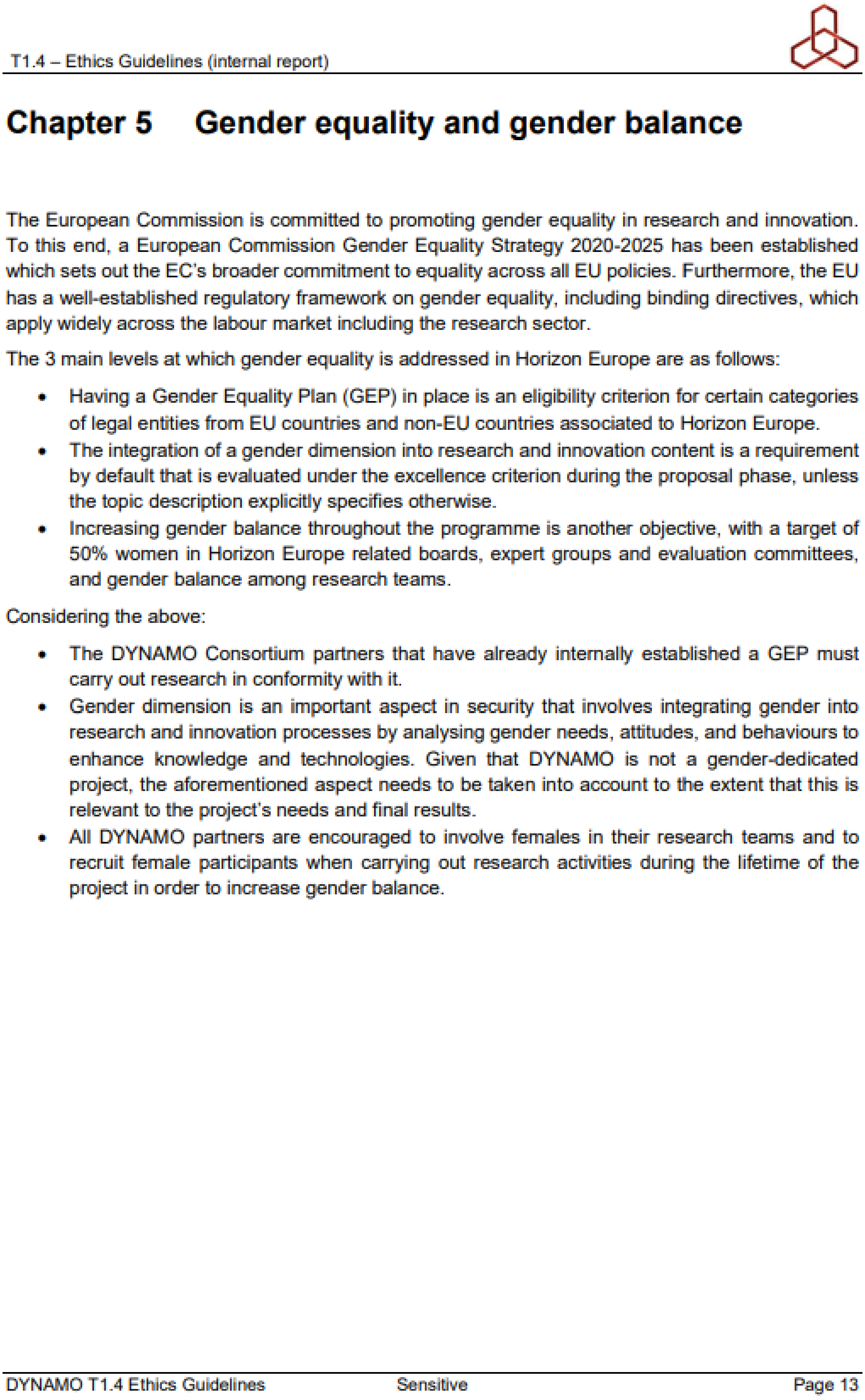
T1.4 – Ethics Guidelines (internal report)

- **Anonymisation or encryption or pseudonymisation of personal data** will be implemented in compliance with the GDPR requirements.
- **DPIAs** will be conducted prior to these data processing operations that are likely to result in high risks for the rights and freedoms of the data subjects.

IMPORTANT NOTES:

1. The **Dissemination & Communication Leader (TEC)** must be **in close collaboration with the Ethics and Legal Advisor (KEMEA) and the Project Coordinator** in order to **filter** the project-related information that is planned to be made available to the public through public dissemination events or publications or through the DYNAMO website and social media accounts and remove any references that are likely to cause misuse of the research results.
2. All Consortium partners need to **identify any relevant risks per task** and the possible malicious events that may occur, to assess their occurrence level, to assess the severity level of the impact, to address the mitigating measures that will be implemented (based on the list above and any additional measures per case) and, finally, to assess the level of their effectiveness. The relevant table can be found on the project's online repository (see WP1 → T1.4 → DYNAMO_MODEL QUESTIONNAIRE_RESEARCH ETHICS_T1.4_for_D1_3 MISUSE.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 12



T1.4 – Ethics Guidelines (internal report)

Chapter 5 Gender equality and gender balance

The European Commission is committed to promoting gender equality in research and innovation. To this end, a European Commission Gender Equality Strategy 2020-2025 has been established which sets out the EC's broader commitment to equality across all EU policies. Furthermore, the EU has a well-established regulatory framework on gender equality, including binding directives, which apply widely across the labour market including the research sector.

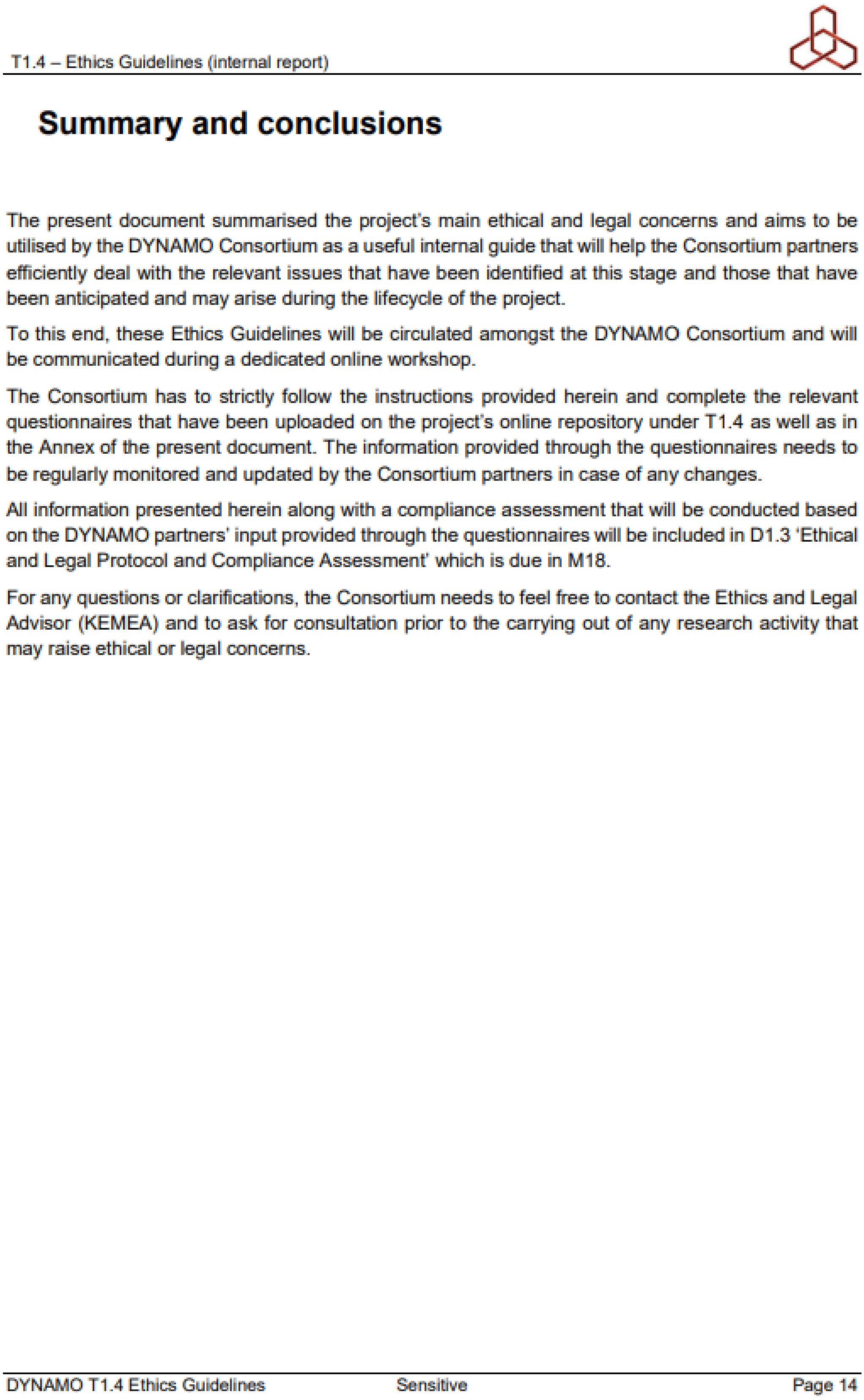
The 3 main levels at which gender equality is addressed in Horizon Europe are as follows:

- Having a Gender Equality Plan (GEP) in place is an eligibility criterion for certain categories of legal entities from EU countries and non-EU countries associated to Horizon Europe.
- The integration of a gender dimension into research and innovation content is a requirement by default that is evaluated under the excellence criterion during the proposal phase, unless the topic description explicitly specifies otherwise.
- Increasing gender balance throughout the programme is another objective, with a target of 50% women in Horizon Europe related boards, expert groups and evaluation committees, and gender balance among research teams.

Considering the above:

- The DYNAMO Consortium partners that have already internally established a GEP must carry out research in conformity with it.
- Gender dimension is an important aspect in security that involves integrating gender into research and innovation processes by analysing gender needs, attitudes, and behaviours to enhance knowledge and technologies. Given that DYNAMO is not a gender-dedicated project, the aforementioned aspect needs to be taken into account to the extent that this is relevant to the project's needs and final results.
- All DYNAMO partners are encouraged to involve females in their research teams and to recruit female participants when carrying out research activities during the lifetime of the project in order to increase gender balance.

DYNAMO T1.4 Ethics Guidelines Sensitive Page 13



Summary and conclusions

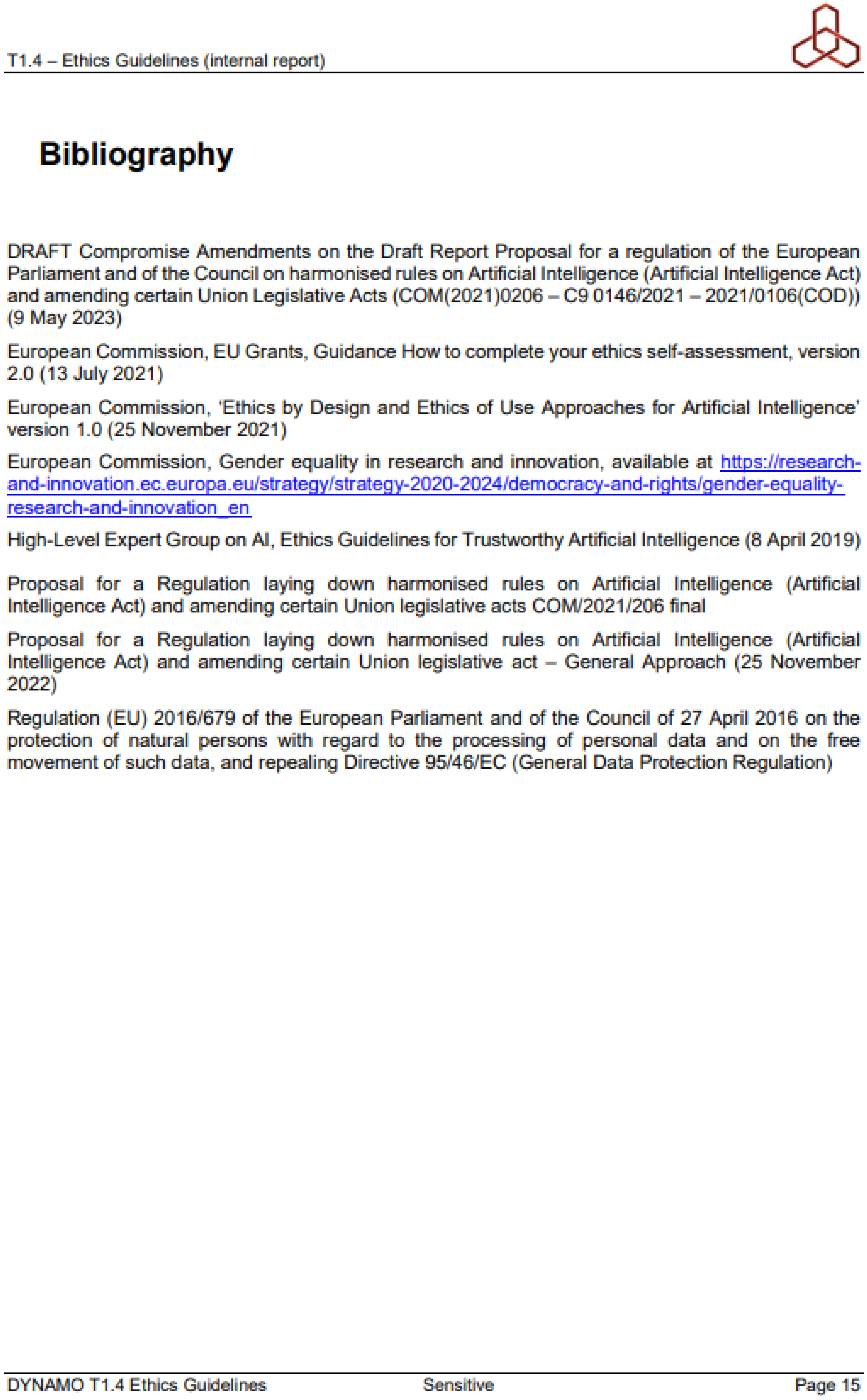
The present document summarised the project's main ethical and legal concerns and aims to be utilised by the DYNAMO Consortium as a useful internal guide that will help the Consortium partners efficiently deal with the relevant issues that have been identified at this stage and those that have been anticipated and may arise during the lifecycle of the project.

To this end, these Ethics Guidelines will be circulated amongst the DYNAMO Consortium and will be communicated during a dedicated online workshop.

The Consortium has to strictly follow the instructions provided herein and complete the relevant questionnaires that have been uploaded on the project's online repository under T1.4 as well as in the Annex of the present document. The information provided through the questionnaires needs to be regularly monitored and updated by the Consortium partners in case of any changes.

All information presented herein along with a compliance assessment that will be conducted based on the DYNAMO partners' input provided through the questionnaires will be included in D1.3 'Ethical and Legal Protocol and Compliance Assessment' which is due in M18.

For any questions or clarifications, the Consortium needs to feel free to contact the Ethics and Legal Advisor (KEMEA) and to ask for consultation prior to the carrying out of any research activity that may raise ethical or legal concerns.



Bibliography

DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)) (9 May 2023)

European Commission, EU Grants, Guidance How to complete your ethics self-assessment, version 2.0 (13 July 2021)

European Commission, 'Ethics by Design and Ethics of Use Approaches for Artificial Intelligence' version 1.0 (25 November 2021)

European Commission, Gender equality in research and innovation, available at https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/democracy-and-rights/gender-equality-research-and-innovation_en

High-Level Expert Group on AI, Ethics Guidelines for Trustworthy Artificial Intelligence (8 April 2019)

Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final

Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative act – General Approach (25 November 2022)

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)