



Project Title	Engaging & supporting EU experts in cybersecurity standardisation activities
Project Acronym	CYBERSTAND.eu
Grant Agreement No.	101158521
Start Date of Project	01.06.2024
Duration of Project	36 months
Project Website	https://cyberstand.eu.eu

D1.2 – Ethics Management and Data Management Plan (EMDMP) |M3|

Work Package	WP1, Project management and coordination
Lead Author (Org)	Luigi Colucci (Trust-IT Services)
Contributing Author(s) (Org)	Nicholas Ferguson (Trust-IT Services), Michele Nannipieri (Trust-IT Services)
Due Date	25.09.2024
Date	04.09.2024
Version	V1.0

Dissemination level

(X) PU: Public

() SEN: Confidential, only for members of the consortium (including the Commission)



Versioning and contribution history

Version	Date	Author	Notes
0.1	02.09.2024	Luigi Colucci & Michele Nannipieri (Trust-IT Services)	ToC and Section 1, 3, 5.
0.2	03.09.2024	Luigi Colucci & Michele Nannipieri (Trust-IT Services)	Section 3, 4.
1.0	04.09.2024	Nicholas Ferguson (Trust-IT Services)	Quality check.

Disclaimer

This document contains information which is proprietary to the CYBERSTAND.eu Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to a third party, in whole or parts, except with the prior consent of the CYBERSTAND.eu Consortium.

Table of contents

1	Introduction	8
2	Ethics Management.....	10
3	Data Management Plan.....	11
3.1	Data summary.....	11
3.1.1	Purpose of the Data Collection/Generation.....	11
3.1.2	Relation to the objectives of the project	11
3.1.3	Types and formats of Data Generated/Collected	12
3.1.4	Existing Data is always on-line and available	12
3.1.5	Origin of the Data	12
3.1.6	Expected size of the Data	12
3.1.7	Data Utility	12
3.1.8	Informed consent form for marketing, and dissemination activities, events and public consultations.....	12
3.2	Making Data findable, including provisions for metadata	13
3.2.1	Discoverability of Data.....	13
3.2.2	Approach towards Search Keywords	13
3.3	Making Data openly accessible	13
3.3.1	Data openly available	13
3.3.2	Methods or Software Tools to Access Data.....	14
3.4	Making Data Interoperable.....	14
3.4.1	Assess the Interoperability of Data	14
3.4.2	Standard Vocabulary for all Data types.....	14
3.5	Increase data re-use (through clarifying licenses).....	14
3.5.1	Data licence to permit the broadest reuse possible	14
3.5.2	Period in which data will be made available for re-use	14
3.5.3	Data Production and Third Parties	15
3.5.4	Data Quality assurance processes	15
3.5.5	Length of time for which the Data will remain re-usable	15
3.6	Allocation of Resources	15
3.6.1	Cost estimation for making data FAIR (findable, accessible, interoperable and reusable) 15	
3.6.2	Responsibilities for Data Management	15
3.6.3	Cost and potential value of long-term preservation	15
3.7	Data Security	16
3.8	Ethical Aspects.....	16
4	Procedures Implemented to support GDPR Compliance.....	17
5	Annexes.....	19
5.1	Privacy Policy.....	19
5.2	Terms of Use	25
5.3	Cookie Policy	27

List of Tables

Table 1 – GDPR procedures and specific functionalities implemented in CYBERSTAND.eu	17
---	----

Terminology

Terminology/Acronym	Description
AE	Affiliated Entity
CA	Consortium Agreement
CMS	Content Management System
CRA	Cyber Resilience Act
CRAWG	Cyber Resilience Act Working Group
CSA	Coordination and Support Action
DCESP	Dissemination, Communication, Engagement, and Sustainability Plan & Report
DEP	Digital Europe Programme
DoA	Description of Action
EC	European Commission
EDIHs	European Digital Innovation Hubs
EE	External Evaluators
ESO	European Standardisation Organisation
EUOS	European Observatory for ICT Standardisation, available at www.standict.eu
GA	Grant Agreement
GDPR	General Data Protection Regulation
KER	Key Exploitable Result
KPI	Key Performance Indicator
NSB	National Standard Body
OA	Open Access
PC	Project Coordinator
PMB	Project Management Board
PO	Project Officer
SB	Strategy Board
SDO	Standards Development Organisation

Terminology/Acronym	Description
SME	Small- and Medium-sized Enterprise
SSPs	Specific Service Procedures
TC	Technical Committee
TGP	Trust Grants Platform
TL	Task Leader
WG	Working Group
WP	Work Package
WPL	Work Package Leader

Executive Summary

This deliverable “D1.2 – Ethics Management and Data Management Plan (EMDMP)” is the formal document that sets out how the data will be handled during the Project duration and beyond.

The DMP therefore provides information on about the following aspects:

- The overall amount and typology of data the Project will generate;
- Ethical and legal compliance of the data;
- Secure storage and data back-up during the lifetime of the project;
- Data preservation and availability for other usages (if appropriate) over the long-term;
- How the project will ensure that data is well organised and adequately documented;
- Distribution of responsibilities for looking after data during and after the project and needed resources.

CYBERSTAND.eu has drawn up this document following the format of the recommended standardised online tool, Dmponline¹, from the Digital Curation Centre in the United Kingdom.

Therefore, the sections in this deliverable follow the suggested template in the Dmponline tool.

As described in the DMP, the data collected by the project comes mainly from the free registration forms on the CYBERSTAND.eu website, for the following purposes:

- To apply to become an External Evaluator (EE);
- To apply for the Specific Service Procedures (SSPs);
- To register for online events such as Webinars or Workshops;
- To receive the CYBERSTAND.eu newsletter.

Emails and passwords are stored in the database of the Drupal Content Management System (CMS) used to build the CYBERSTAND.eu website and are not shared with anyone outside of the Project.

This information is used to send targeted communications to our community of users, such as newsletters, invitations to webinars and other events, and similar activities aimed at community development and engagement.

Overall, CYBERSTAND.eu is in full compliance with the provision of General Data Protection Regulation (GDPR) which has been in force across Europe since 25th of May, 2018.

¹ <https://www.dcc.ac.uk/dmponline>

1 Introduction

This deliverable “D1.2 – Ethics Management and Data Management Plan (EMDMP)”, released at Month 3, provides information on our ethics management and an DMP which involves the data structure and capture activities involved in the CYBERSTAND.eu’s web platform.

Additionally, the deliverable outlines the data the CYBERSTAND.eu consortium is expected to acquire and generate during the project, including how it will be managed, described, analysed, and stored.

It also details the mechanisms that will be applied at the project's end to share and preserve the data.

This report mainly deals with the activities and project deliverables managed under:

- WP2 – Pan-European standardisation efforts supporting implementation of the CRA;
- WP3 – Support to EU standardisation experts (SSPs).
- WP4 - Communication & dissemination, engagement, training, and sustainability.

The related deliverables of WP2 are:

- D2.1 – Prioritisation of CRA Work Items;
- D2.2 – First release of White paper;
- D2.3 – CRA & Policy Regulations;
- D2.4 – Second & Final Release of White paper.

The related deliverables of WP3 are:

- D3.1 – Experts’ application package;
- D3.2 – Monitoring & impact (1st period);
- D3.3 – Monitoring & impact (2nd period).

The related deliverables of WP4 are:

- D4.1 – Dissemination, Communication, Engagement, and Sustainability Plan & Report First release
- D3.2 – Dissemination, Communication, Engagement, and Sustainability Plan & Report (mid-term release)
- D3.3 – Dissemination, Communication, Engagement, and Sustainability Plan & Report DCESP (final release)
- D4.4 - Events, Workshop and Webinar 1st yearly report
- D4.5 - Events, Workshop and Webinar 2nd yearly report
- D4.6 - Events, Workshop and Webinar 2nd yearly report
- D4.7 Sustainability strategy
- D4.8 - SME engagement and consultation report – interim version
- D4.9 - SME engagement and consultation report – final version

The document is organised as follows:

- Section 2 is focused on the Ethics Management of CYBERSTAND.eu;
- Section 3 addresses all the items required in the Data Management Plan in compliance with the table of contents of the Dmponline tool;

- Section 4 summarises the procedures followed by CYBERSTAND.eu to comply with the GDPR.

2 Ethics Management

This section of the DMP includes ethical aspects, values and information on data protection in the context of the project that might affect data sharing.

CYBERSTAND.eu reaches out to many organisations, individuals, and other projects, and organises interviews (video recordings and multimedia content creation), workshops, and other activities, involving people from within and outside the project. In doing so CYBERSTAND.eu ensures proper handling of ethical aspects, values, and data protection in accordance with articles 14 and 15 of the Grant Agreement.

While each partner is responsible for their own actions, Trust-IT as coordinator of the CYBERSTAND.eu project directs and supports partners in acting according to the DMP. CYBERSTAND.eu has a Privacy Policy and Terms of Use Statement for services provided via the project website, which addresses personal data (processing, data subject's rights, opt-out, cookies used on the website and in social media, etc.).

Trust-IT acts as the Data Controller for all personal data processing conducted through the website, while all project partners are designated as Data Processors under the General Data Protection Regulation (GDPR). As such, they are authorised to access personal data provided via the website managed by Trust-IT. For example, Name, contact details and other Personal Data (email, sensitive information, e.g. regarding gender) processed for applications collected via the CYBERSTAND.eu website will be kept by Trust-IT as Data Controller for up to 5 years, to allow for possible external audits, as requested by contractual provisions the Data Controller is subjected to and also to support sustainability of the project outputs.

The project only collects personal data that is necessary to fulfil its information needs, respecting the principle of data minimisation, and will not intentionally collect “special categories of data” in terms of the GDPR. All personal data collected for the project will be processed in accordance with the GDPR. When requesting non-mandatory personal information from the user through the CYBERSTAND.eu website, information disclaimers are included to clarify the usage of the info, for statistics purposes and improve service delivery.

A large part of the personal data is collected through the CYBERSTAND.eu website which offers a privacy statement. Through the website a so-called data subject can register for the newsletter, mailing lists and events. These processes are based on informed consent that is gathered through the website. The other main means of gathering information is through interviews. Processing this information is again based on informed consent, where data subjects are properly informed on, among other things, the purposes of the data collection, how the data will be used, and with whom it may be shared.

For interviews the project utilises specific templates for informed consent forms and information sheets (in language and terms intelligible to the participants). Personal data of the project partners for purposes of administering the project activities will not be shared externally unless there is a sufficiently substantiated reason to do so.

The CYBERSTAND.eu website and its contacts' database are managed by the CYBERSTAND.eu WP 4 leader for “Communication & dissemination, engagement, training, and sustainability”, Trust-IT.

3 Data Management Plan

3.1 Data summary

3.1.1 Purpose of the Data Collection/Generation

At the core of CYBERSTAND.eu's architecture is the SSP Platform. This is accessible to registrants through a personalised Dashboard accessed via the project website <https://cyberstand.eu/>. The platform provides and manages the processes related to the six Specific Service Procedure (SSP).

The main features of the SSP Platform are:

- SSP application platform, where applicants can enter and submit proposal for each of the six SSPs of the project.
- External Evaluators (EEs) application form, where applicants can apply to become one of CYBERSTAND.eu expert evaluators.
- The Evaluation Workflow where the EEs carry out the assessment of each proposal submitted to the selection procedures.

The “Dashboard” is only available to the user once they are logged in, and is dependent on user privileges and rights attributed on the basis on their role within the Project.

When registering as a platform user, the participant must accept the platform privacy policy. This Privacy policy is fully GDPR compliant, may be amended during the project lifetime and can be viewed at <https://cyberstand.eu/privacy-policy> (see Annex – PRIVACY POLICY)

CYBERSTAND.eu collects the registered email address only to verify the account. In addition, during this initial registration process, the user is given an option to “opt-in” to the CYBERSTAND.eu newsletter mailing list and to receive automatic and manually generated emails regarding the SSP and their specific roles and tasks.

It is expected that there will be occasional surveys and public consultations undertaken for gathering feedback on the platform and these will be optional. The source data is not made public or shared outside the consortium. This data is used to generate summary reports only.

3.1.2 Relation to the objectives of the project

The CYBERSTAND.eu project has four key-objectives:

- Deliver a coherent and engaging series of events and publications to establish an inclusive community of cybersecurity experts;
- Establish a facility dedicated to support EU experts contributing to standardisation efforts, in EU an Int'l cybersecurity standardisation;
- Foster the development on harmonised standards, in conformity with the Cyber Resilience Act (CRA);
- Contributing to implementation of European Values and sustainability of the CRA.

Since all these objectives relate to the methodology for collection of information from stakeholders during and after the project, they are all to a certain degree related to the topic of data collection and generation.

3.1.3 Types and formats of Data Generated/Collected

Users enter the data directly into the SSP Platform, guided by form fields and help guides that specify the expected format and length for each entry.

3.1.4 Existing Data is always on-line and available

As mentioned above, the users are given dedicated and customised privileges, dependent on their role, and the information is always on-line and available, when needed.

The source data from feedback surveys undertaken is not made public or shared outside the consortium. It is only used by the consortium for the purposes of gathering feedback to help improve the platform for future open calls.

3.1.5 Origin of the Data

In the case of user entry, the data is provided by the platform users themselves. The data will not be interfered with by any other users. As mentioned above, the users are given dedicated and customised privileges, based on their role.

3.1.6 Expected size of the Data

The entries to the SSP Platform are guided for each field of entry required. The data could range from tick-boxes, to single word categories to fields that would require up to maximum 1,000 words length.

In total over the lifetime of the project, it is expected that the entire data will not be more than 1GB. Personal data will form no larger than 100 MB (based on 20,000 users each with 50kB of personal data).

3.1.7 Data Utility

All the information gathered by the SSP Platform is to support the CYBERSTAND.eu project, the European Commission and the international community of researchers. This data will assist with applying for funding, having applications evaluated and selected in a timely and efficient manner during the six SSPs of the project.

If needed, survey data for gathering feedback on the platform consisting of anonymised summary reports to assist the consortium to improve the platform for future calls will be gathered. The data will be collected without using the personal data of the user. The personal data of the users is not shared beyond the Project consortium members and EE members for the assigned proposals only.

3.1.8 Informed consent form for marketing, and dissemination activities, events and public consultations

All users will be informed of the Privacy Policy and Terms of Use of the CYBERSTAND.eu portal during registration, and consent will be provided by accepting and completing the registration form.

3.2 Making Data findable, including provisions for metadata

3.2.1 Discoverability of Data

The SSP Platform has been designed to allow the users to find their applications when they have logged into the system. Their level of discoverability is tailored and dependent on their privileges as a user, as follows:

- SSP applicants: once logged in, they will have access to their own profiles and access to the current status of the proposals to keep track of any potential update;
- External Evaluators (EEs) applicants: they will have access to both an “Applications” and the “My Applications” buttons. When the user logs in for the first time, they are given a choice to submit an application as an EE or for the SSPss. If they submit an application and are accepted onto the EEs, the “My Applications” button will show their EEs application and the “Applications” button will show the applications assigned to them to evaluate;
- Selected and assigned EE members: following the deadline of the call and once the submitted applications are assigned to the EE members for evaluation, upon login they are given access only to the proposals they are assigned to evaluate or to perform Quality Control.

3.2.2 Approach towards Search Keywords

The SSP Platform is equipped with a search functionality that is mostly used to find specific proposals more easily and/or users/applicants.

Approach for clear versioning

The SSP platform entries are date and time stamped, which will enable clear versioning of the entries themselves and reports can be generated, when needed (e.g. for purposes of gathering anonymised statistics, as required by the European Commission).

3.3 Making Data openly accessible

3.3.1 Data openly available

The textual and graphical data entered by the end users into the SSP platform in relation to the applications is only available on a need-to-know basis, and privilege basis. The data will be made available in two forms:

- The data entries themselves are openly available on the SSP platform itself, only for those with the privileges to view them;
- A PDF file of the contract will be shared with the funded applicant(s). Only personal data required in relation to capturing the identity of the signatories within the contract will be included in this output.

3.3.2 Methods or Software Tools to Access Data

The CYBERSTAND.eu platform has been developed using Drupal, a powerful CMS (Content Management System), that allows a modern look and an appealing UX design. This platform was chosen since it has standard features that are functional and easy to use, such as content authoring, reliable performance, and excellent security. The Drupal Platform (made in PHP language) was found to be extremely flexible and modular, necessary for the purposes of the CYBERSTAND.eu platform. The entire platform is designed with a user-centric layout to facilitate access to the content and usability of the portal. Finally, the Drupal platform is a well-suited base to develop a GDPR-compliant TGP, which is one of the main goals of the CYBERSTAND.eu initiative.

3.4 Making Data Interoperable

3.4.1 Assess the Interoperability of Data

The data from the CYBERSTAND.eu platform will not be shared with third parties for any reason, except for our own anonymous statistical data. Therefore, the interoperability aspects of the data are not considered by the project.

3.4.2 Standard Vocabulary for all Data types

During the data entry process, the project team provides guidance to the users for data entry in terms of standard vocabulary and size of entries (number of characters or words) for all data types.

3.5 Increase data re-use (through clarifying licenses)

3.5.1 Data licence to permit the broadest reuse possible

When users register, they accept a terms and conditions of usage, where it is made clear that data added to the platform will not be publicly available, including their personal data.

3.5.2 Period in which data will be made available for re-use

The information and data input to the platform will only be regularly downloaded in an anonymised way (with no personal data) and summarised to be used for generating statistics, for monitoring the results of the open calls, such as number of applications submitted, where applicable. This will include data such as number of proposals submitted, number of funded proposals, number of different organisation types involved, total budget requested, typology of requested funds, and geographical provenance of the applicants.

From the perspective of open data available for re-use, as the project has recently started, we recognise that as the ongoing process develops over the project lifetime, it is our plan to review the type of data generated and which data belongs where in order to update the DMP, if necessary.

3.5.3 Data Production and Third Parties

Apart from the EE members assigned to evaluate the individual proposals and the proposers themselves, the data collected will not be available, at any time, for usability by any other third parties, under any circumstances, unless it is anonymised, such as the statistical data mentioned above.

3.5.4 Data Quality assurance processes

The PMB which is comprised of members from each consortium partner of CYBERSTAND.eu and whose responsibilities includes all aspects regarding notifications for meetings, voting, quorum and formalisation of all decisions, will monitor the data with this important consideration in mind on a regular basis to ensure that the quality of the data is taken into consideration.

3.5.5 Length of time for which the Data will remain re-usable

It is expected that the data will remain re-usable for the lifetime of this project only. It is possible that the project may need to maintain the data beyond the end date of the Project, should the records of the Project need to be kept for review purposes by the European Commission services and independent evaluators, for a specific duration after the project is officially concluded. This duration would be based upon the specific requirement placed upon the CYBERSTAND.eu Project by the Commission as to storing the data after Project Conclusion.

3.6 Allocation of Resources

3.6.1 Cost estimation for making data FAIR (findable, accessible, interoperable and reusable)

The costs associated with the data is considered low, as the system has already been designed as GDPR compliant and uses tools that are both user friendly and provide the developers with ease of access for moderation. The efforts associated with ensuring the data is FAIR is taken care of primarily in the personnel costs of the project.

3.6.2 Responsibilities for Data Management

The overall data management in the project is the responsibility of WP1, “Project management and coordination”, in close conjunction with the WP and task leaders in WP2, “Support to EU standardisation experts and impact monitoring”.

In addition, there are regular discussions in the bi-weekly CYBERSTAND.eu PMB Meetings about the overall data management. Trust-IT is the data controller for all data collected under the project. The Data Processing Officer for Trust-IT is:

Mr. Michele Nannipieri, m.nannipieri@trust-itservices.com

3.6.3 Cost and potential value of long-term preservation

The costs involved and potential value would be considered relatively low, as the preservation of the data is not expected to be long term.

3.7 Data Security

The overall Platform adopts security measures consistent with the provisions of the General Data Protection Regulation (GDPR) to protect personal information under its control against loss, misuse, and alteration.

In general terms, server configuration, https certificates, access controls, password storage and other relevant elements are dealt with in accordance to the provisions of the GDPR.

We attempt to strike a reasonable balance between security and convenience. Emails are usually sent as unencrypted text. If misrouted or intercepted, an unencrypted email could be read easily. If a matter requires high security or confidentiality, partners are asked to inform Trust-IT about the sensitivity of the information and have been advised not to send it via email.

The Project will take measures to prevent data loss and facilitate any security aspects related to the transfer of data and information, as required.

3.8 Ethical Aspects

This project involves the collection of data from human participants and acts as the online portal streamlining the CYBERSTAND.eu application process.

While we consider that ethical approvals may not be needed, we agree that the project is not free of ethical considerations. We identify the following, according to the ethics Horizon 2020 Programme Guidance on ethics self-assessment in H2020²:

- Confirm that informed consent has been obtained. Yes, it was obtained when the user registered to the site and agreed to the privacy policy. Consent for any information that will be made open access will also be obtained;
- Documents to be provided/kept on file: Informed Consent Forms and Information Sheets. These records are kept on record on the website server, and can be inspected, if requested.

² h2020_hi_ethics-self-assess_en.pdf (europa.eu)

4 Procedures Implemented to support GDPR Compliance

The following procedures and specific functionalities have been implemented and are continuously maintained to ensure compliance to the GDPR:

Table 1 – GDPR procedures and specific functionalities implemented in CYBERSTAND.eu

GDPR main points	Typical Drupal website installation
The right to be informed	Privacy notice webpage.
The right of access	Usually, all user data are accessible after login.
The right to rectification	Usually, all data are editable by the user.
The right to erasure	It is possible to delete user account.
The right to restrict processing	It is possible to disable user account, non-personal data generated by the user will be still visible but can't be changed anymore.
The right to data portability	It is possible to provide data export in CSV format.
The right to object	<p>In the privacy notice:</p> <ul style="list-style-type: none"> You must inform individuals of their right to object “at the point of first communication” and in your privacy notice. This must be “explicitly brought to the attention of the data subject and shall be presented clearly and SSParately from any other information”.
Rights related to automated decision making and profiling	Usually, no automated processing of personal data on Drupal.
Accountability and governance	<ul style="list-style-type: none"> Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies. Maintain relevant documentation on processing activities. Where appropriate, appoint a data protection officer. Implement measures that meet the principles of data protection by design and data protection by default. Measures could include: <ul style="list-style-type: none"> Data minimisation; Pseudonymisation; Transparency; Allowing individuals to monitor processing; and Creating and improving security features on an ongoing basis.

	<ul style="list-style-type: none"> • Use data protection impact assessments where appropriate.
Breach notification	You only must notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

In case of data breach, the notification will be sent within 72 hours to Commission de la protection de la vie privée, Rue de la Presse, 35, 1000 Bruxelles³.

³ <https://www.privacycommission.be/fr/politique-vie-privee-et-disclaimer>

5 Annexes

5.1 Privacy Policy

The Data Controller is Trust-IT Services srl ("Trust-IT"), with registered offices in Via Francesco Redi 10, 56124 Pisa, VAT no. and Fiscal Code P.I. e C.F. 01870130505, is committed to protecting the online privacy of the users of this website ("Website").

As such, this Privacy Policy has been written to allow you to understand Trust-it's policy regarding your privacy, as well as how your personal information will be handled when using the Website. This Privacy Policy will also provide you with information so that you are able to consent to the processing of your personal data in an explicit and informed manner, where appropriate.

In general, any information and data which you provide to Trust-it over the Website, or which is otherwise gathered via the Website by Trust-it, in the context of the use of Website's services ("Services") as better defined in Section 3 below, will be processed by Trust-it in a lawful, fair and transparent manner. To this end, and as further described below, Trust-it takes into consideration internationally recognised principles governing the processing of personal data, such as purpose limitation, storage limitation, data minimisation, data quality and confidentiality.

1. Data controller

Trust-IT, as identified at the top of this Privacy Policy, is the data controller regarding all personal data processing carried out through the Website. You can contact Trust-IT with any questions related to this Privacy Policy or the Trust-IT's personal data processing practices by sending a written communication to web@cyberstand.eu, or via the contact forms available on the Website.

2. Personal Data processed

When you use the Website, Trust-it will collect and process information regarding you (as an individual) which allows you to be identified either by itself, or together with other information which has been collected. Trust-it may also be able to collect and process information regarding other persons in this same manner, if you choose to provide it to Trust-it, also via the Website.

This information may be classified as "Personal Data" and can be collected by Trust-it both when you choose to provide it (e.g., when you subscribe to the newsletter or request other Services provided by Trust-it over the Website) or simply by analysing your behaviour on the Website.

Personal Data which can be processed by Trust-it through the Website are as follows:

a. Name, contact details and other Personal Data

In various areas of the Website – including, in particular, if you decide to create an account on the Website – you will be asked to submit information about yourself, such as your name, professional title, organisation name/type, primary (and secondary) domain of work/expertise, e-mail address, city/country of residence, address, gender, Twitter handle, LinkedIn profile, and picture. Mandatory fields will be marked as such in the online registration forms – it is not possible to process your registration if any of the mandatory fields are left incomplete.

In addition, whenever you communicate with Trust-it by submitting a general enquiry or a support ticket via the Website, as well as whenever you participate in surveys which may be available on the Website, Trust-it may collect additional information which you choose to provide.

Regarding any applications received, Trust-it may assess the professional social media accounts (e.g. LinkedIn, Twitter) or professional websites of candidates, where publicly available or

disclosed by the candidate, as necessary to gain insight as to a candidate's suitability for the position/function to which the candidate applied.

When signing up for an event via the Website (such as a workshop organised or promoted by the Website), you will also be asked to provide details such as your name, your Twitter handle, the dates on which you will be attending and other information of relevance for the management of your attendance. Your payment details (including debit/credit card number and bank account details as needed) will be processed via an external payment gateway.

b. Special categories of Personal Data

When signing up for an event via the Website (such as a workshop organised or promoted by the Website), you will also be asked whether you have any special dietary/access requirements which might need accommodation. These Personal Data may potentially qualify as "health data" or "data revealing your religious/philosophical beliefs", which are special categories of personal data under Art. 9 GDPR, and will be processed only with your explicit consent.

Certain areas of the Website may include free text fields, where you can write messages to Trust-it or otherwise allow you to post various types of content on the Website, which may contain Personal Data. Where these fields are completely free, you may use them to disclose (inadvertently or not) more sensitive categories of Personal Data, such as data revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. The content you upload in these fields may also (inadvertently or not) include other types of sensitive information relating to you, such as your genetic data, biometric data or data concerning your health, sex life or sexual orientation.

Trust-it asks that you do not disclose any sensitive Personal Data on the Website, unless you consider this to be strictly necessary. As it is totally optional to provide this information, if you nonetheless choose to do so, please mind that Trust-it requires your explicit consent to process this sort of Personal Data (which can be provided, e.g., by declaring that you "explicitly consent to the processing of my special categories of personal data for the purpose of assessing my candidacy").

c. Other persons' Personal Data

As mentioned in the previous section, certain areas of the Website include free text fields where you can write messages to Trust-it, or otherwise allow you to post various types of content on the Website. These messages and content may (inadvertently or not) include Personal Data related to other persons.

In any situation where you decide to share Personal Data related to other persons, you will be considered as an independent data controller regarding that Personal Data and must assume all inherent legal obligations and responsibilities. This means, among other things, that you must fully indemnify Trust-it against any complaints, claims or demands for compensation for damages which may arise from the processing of this Personal Data, brought by the third parties whose information you provide through the Website.

As Trust-it does not collect this information directly from these third parties (but rather collects them, indirectly, from you), you must make sure that you have these third parties' consent before providing any information regarding them to Trust-it; if not, then you must make sure there is some other appropriate grounds on which you can rely to lawfully give Trust-it this information.

d. Browsing data

The Website's operation, as is standard with any websites on the Internet, involves the use of computer systems and software procedures, which collect information about the Website's users

as part of their routine operation. While Trust-it does not collect this information in order to link it to specific users, it is still possible to identify those users either directly via that information, or by using other information collected – as such, this information must also be considered Personal Data.

This information includes several parameters related to your operating system and IT environment, including your IP address, location (country), the domain names of your device, the type of device, the URI (Uniform Resource Identifier) addresses of resources you request on the Website, the time of requests made, the method used to submit requests to the server, the dimensions of the file obtained in response to a request, the numerical code indicating the status of the response sent by the server (successful, error, etc.), and so on.

These data are used to compile statistical information on the use of the Website, to ensure its correct operation, as well as restore backup from possible failures of the Website and identify any faults and/or abuse of the Website. Save for this last purpose, these data are not kept for more than 60 business days.

e. Cookies

- Definitions, characteristics, and application of standards

Cookies are small text files that may be sent to and registered on your computer by the websites you visit, to then be re-sent to those same sites when you visit them again. It is thanks to these cookies that those websites can “remember” your actions and preferences (e.g., login data, language, font size, other display settings, etc.), so that you do not need to configure them again when you next visit the website, or when you change pages within a website.

Cookies are used for electronic authentication, monitoring of sessions and storage of information regarding your activities when accessing a website. They may also contain a unique ID code which allows tracking of your browsing activities within a website, for statistical or advertising purposes. Some operations within a website may not be able to be performed without the use of cookies which, in certain cases, are technically necessary for operation of the website.

When browsing a website, you may also receive cookies from websites or web servers other than the website being visited (i.e., “third-party cookies”).

There are various types of cookies, depending on their characteristics and functions, which may be stored on your computer for different periods of time: “session cookies”, which are automatically deleted when you close your browser, and “persistent cookies”, which will remain on your device until their pre-set expiration period passes.

According to the law which may be applicable to you, your consent may not always be necessary for cookies to be used on a website. In particular, “technical cookies” – i.e. cookies which are only used to send messages through an electronic communications network, or which are needed to provide services you request – typically do not require this consent. This includes browsing or session cookies (used to allow users to login) and function cookies (used to remember choices made by a user when accessing the website, such as language or products selected for purchase).

- Types of cookies used by the Website

The Website uses the following types of cookies:

Browsing or session cookies, which are strictly necessary for the Website’s operation, and/or to allow you to use the Website’s content and Services.

Analytics cookies, which allow Trust-it to understand how users make use of the Website, and to track traffic to and from the Website.

Trust-it also uses third-party cookies – i.e. cookies from websites / web servers other than the Website, owned by third parties. These third parties will either act as independent data controllers from Trust-it regarding their own cookies (using the data they collect for their own purposes and under terms defined by them) or as data processors for Trust-it (processing personal data on Trust-it's behalf).

For further information on how these third parties may use your information, please refer to their privacy policies:

Twitter

LinkedIn

The list of installed cookies is available in the Cookie Policy on the Website

- Cookie settings

You can block or delete cookies used on the Website via your browser options. Your cookie preferences will be reset if different browsers are used to access the Website. For more information on how to set the preferences for cookies via your browser, please refer to the following instructions:

[Chrome](#)

[Firefox](#)

[Internet Explorer](#)

[Safari](#)

You may also provide set your preferences on third-party cookies by using online platforms such as AdChoice.

CAUTION If you block or delete technical and/or function cookies used by the Website, the Website may become impossible to browse, certain services or functions of the Website may become unavailable or other malfunctions may occur. In this case, you may have to modify or manually enter some information or preferences every time you visit the Website.

3. Purposes of processing

Trust-it intends to use your Personal Data, collected through the Website, for the following purposes:

1. To allow you to create and maintain a registered user profile on the Website, to allow you to participate in different areas over the Website and exchange information/documents with other participants, to verify your identity and assist you, in case you lose or forget your login / password details for any of the Website's registration services, to send you informative newsletters and other communications (linked to the collaborative areas which you participate in), to respond to your enquiries and requests for support, and to provide any other Services which you may request ("Service Provision");
2. To process your sign-up/registration forms for events and webinars hosted or supported by the Website, process your payment details for associated fees, track event attendance and publish attendee lists online ("Events/Webinars");
3. To assess applications submitted via the Website, such as collaborating opportunities or for participating to events organised or sponsored by the Website, among others ("Applications");
4. For compliance with laws which impose upon Trust-it the collection and/or further processing of certain kinds of Personal Data ("Compliance");

5. For development and administration of the Website, in particular by use of data analytics regarding how you and other users make use of the Website, as well as the information and feedback you provide, to improve our offerings (“Analytics”);

6. To prevent and detect any misuse of the Website, or any fraudulent activities carried out through the Website, including by carrying out internal audits (“Misuse/Fraud”).

4. Grounds for processing and mandatory / discretionary nature of processing

Trust-it’s legal bases to process your Personal Data, according to the purposes identified in Section 3, are as follows:

1. Service Provision: processing for these purposes is necessary to provide the Services and, therefore, is necessary for the performance of a contract with you – Art. 6(1)(b) GDPR. It is not mandatory for you to give Trust-it your Personal Data for these purposes; however, if you do not, Trust-it will not be able to provide any Services to you.

2. Events/Webinars: processing for these purposes is generally necessary to allow the Trust-it Team to respond to your request to sign up for an event/webinar and, therefore, is necessary for the performance of a contract with you – Art. 6(1)(b) GDPR. However, the tracking of event attendance and publication of attendee lists is done on the basis of the Website’s interests in managing events and allowing other participants to become aware of persons taking part at the event – Art. 6(1)(f) GDPR. It is not mandatory for you to give Trust-it your Personal Data for these purposes; however, if you do not, Trust-it will not be able to process your registration for an event/webinar.

3. Applications: processing for this purpose is needed in order for Trust-it to be able to consider your application and, therefore, is necessary to take steps at your request before (potentially) entering into a contract – Art. 6(1)(b) GDPR. It is not mandatory for you to give Trust-it your Personal Data for these purposes; however, if you do not, Trust-it will not be able to consider your applications.

4. Compliance: processing for this purpose is necessary for Trust-it to comply with its legal obligations – Art. 6(1)(c) GDPR. When you provide any Personal Data to Trust-it, Trust-it must process it in accordance with the laws applicable to it, which may include retaining and reporting your Personal Data to official authorities for compliance with tax, customs or other legal obligations.

5. Analytics: Information collected for this purpose is used to allow Trust-it to understand how users interact with the Website and to improve the Website accordingly, with the aim to providing a better user experience – Art. 6(1)(f) GDPR.

6. Misuse/Fraud: Information collected for this purpose is used exclusively to prevent and detect fraudulent activities or misuse of the Website (for potentially criminal purposes) – Art. 6(1)(f) GDPR.

5. Recipients of Personal Data – Data Processors

Your Personal Data may be shared with the following list of entities (“Data Processors”):

The following entities are engaged in order to provide or support the Website and Services (e.g., hosting providers, e-mail platform providers, technical maintenance providers Website administrators and Website user administrators):

EUROPEAN CYBER SECURITY ORGANISATION, (ECSO), beneficiary, with legal address in 1000 Avenue Des Arts 46, Bruxelles, 1000, Belgium

EUROPEAN DIGITAL SME ALLIANCE, (DSME), beneficiary, with legal address in Rue Marie Therese, 21/5, Bruxelles, 1000, Belgium

COMITE EUROPEEN DE NORMALISATION, (CEN), beneficiary, with legal address in Rue De La Science, 23, Bruxelles, 1040, Belgium

COMITE EUROPEEN DE NORMALISATION ELECTROTECHNIQUE, (CENELEC), beneficiary, with legal address in Rue De La Science, 23, Bruxelles, 1040, Belgium

INSTITUT EUROPEEN DES NORMES DE TELECOMMUNICATION ASSOCIATION, (ETSI), beneficiary, with legal address in Rue Des Lucioles, Sophia Cedex, 06921, France

Commpla Srl - Via Francesco Redi 10, 56124 Pisa- Italy P IVA 01958380501 Data Processor email: info@commpla.com

The Rocket Science Group LLC d/b/a Mailchimp, 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308 USA, dpo@mailchimp.com

Zoom Video Communications, Inc., 55 Almaden Blvd, Suite 600, San Jose, CA 95113, managing webinar service with Personal Data Residency in Europe

Google Ireland Limited; Gordon House Barrow Street, Dublin 4 DUBLIN, D04 E5W5 Ireland, managing the Google Analytics service for European-based websites

6. Other Recipients of Personal Data

Your Personal Data may be shared with the following list of persons / entities ("Recipients"):

Persons, companies or professional firms providing the Trust-it with advice and consultancy regarding accounting, administrative, legal, tax, financial and debt collection matters related to the provision of the Services and which act typically as data processors on behalf of the Trust-it;

Persons authorised by Trust-it to process Personal Data needed to carry out activities strictly related to the provision of the Services, who have undertaken an obligation of confidentiality or are subject to an appropriate legal obligation of confidentiality (e.g., members of the team operating the Website, and other functions with access to Personal Data processed via the Website);

Public entities, bodies or authorities to whom your Personal Data may be disclosed, in accordance with the applicable law or binding orders of those entities, bodies or authorities.

Additionally, with your consent, some of your Personal Data may be published in the webpages available online at the Website. Furthermore, when you sign-up for an event, you will be listed in attendee lists made available on the Website.

More information on these transfers is available upon written request to the Website Managing Team at the following address: web@cyberstand.eu.

7. Retention of Personal Data

Personal Data processed for Service Provision and Events/Webinars will be kept by Trust-it for the period deemed strictly necessary to fulfil such purposes – in any case, as these Personal Data are processed for the provision of the Services, Trust-it may continue to store this Personal Data for a longer period, as may be necessary to protect Trust-it's interests related to potential liability related to the provision of the Services.

Personal Data processed for Applications will be kept by Trust-it for up to 5 years. Trust-it may contact applicants before the expiration of this period, in order to request an extension of the retention period.

Personal Data processed for Compliance will be kept by Trust-it for the period required by the specific legal obligation or by the applicable law.

Personal Data processed for preventing Misuse/Fraud will be kept by Trust-it for as long as deemed strictly necessary to fulfil the purposes for which it was collected.

More information on applicable retention periods is available upon written request to the Website Managing Team at the following address: web@cyberstand.eu.

8. Data subjects' rights

As a data subject, you are entitled to exercise the following rights before Trust-it, at any time:

1. Access your Personal Data being processed by Trust-it (and/or a copy of that Personal Data), as well as information on the processing of your Personal Data;
2. Correct or update your Personal Data processed by Trust-it, where it may be inaccurate or incomplete;
3. Request erasure of your Personal Data being processed by Trust-it, where you feel that the processing is unnecessary or otherwise unlawful;
4. Request the restriction of the processing of your Personal Data, where you feel that the Personal Data processed is inaccurate, unnecessary or unlawfully processed, or where you have objected to the processing;
5. Exercise your right to portability: the right to obtain a copy of your Personal Data provided to Trust-it, in a structured, commonly used and machine-readable format, as well as the transmission of that Personal Data to another data controller;
6. Object to the processing of your Personal Data, based on relevant grounds related to your particular situation, which you believe must prevent Trust-it from processing your Personal Data;

Please note that most of the Personal Data you provide to Trust-it can be changed at any time, including your e-mail preferences, by accessing, where applicable, your user profile created on the Website.

Aside from the above means, you can always exercise your rights described above by sending a written request to the Website Managing Team at the following address: web@cyberstand.eu.

In any case, please note that, as a data subject, you are entitled to file a complaint with the competent supervisory authorities for the protection of Personal Data, if you believe that the processing of your Personal Data carried out through the Website is unlawful.

9. Amendments

This Privacy Policy entered into force on 01/07/2024

Trust-it reserves the right to partly or fully amend this Privacy Policy, or simply to update its content, e.g., as a result of changes in applicable law. The Website Managing Team will inform you of such changes as soon as they are introduced, and they will be binding as soon as they are published on the Website. The Website Managing Team therefore invites you to regularly visit this Privacy Policy in order to acquaint yourself with the latest, updated version of the Privacy Policy, so that you may remain constantly informed on how Trust-it collects and uses Personal Data.

5.2 Terms of Use

These Terms of Use are applicable to all users of this website ("Website"). Users should read, understand and accept these Terms when creating an account on the Website or using any of the services provided via this Website. If a given user has not done this, or does not agree with the

contents of these Terms of Use, that user should not create an account on the Website and should not make use of any of the services provided via this Website.

By accepting these Terms of Use, upon creation of an account on the Website, the user enters into an agreement with Trust-it, with registered offices at Trust-it SRL, with registered offices in Via Francesco Redi 10, 56124 Pisa - P.I. e C.F. 01870130505 ("Trust-it"), made up by the contents of these Terms, in order to regulate the user's access and use of the Website. Users which accept these Terms of Use hereby represent and warrant that:

They accept to be bound by these Terms of Use, as registered Website users – either individually, or in representation of an organisation;

They are at least 18 years old;

They are capable, under the terms of the law applicable to them, to be legally bound by and comply with these Terms of Use – in particular, whenever a user creates an account as a representative of an organisation, that user warrants to have been expressly and validly authorised by that organisation to do so, or to otherwise be a legitimate representative of that organisation under the applicable law;

Their use of the Website will be carried out in accordance with all applicable laws and regulations.

In the event of doubts concerning the Terms of Use, Trust-it may be contacted at: web@cyberstand.eu.

For information on the processing of personal data on users which is carried out via the Website, please see the /privacy-policy

1. Services provided via the Website

Access to services provided via the Website ("Services") is, in part, restricted to registered users – i.e., users with a registered Website account – although some Services are open to all Website users. The creation of an account and access to the Website is generally free of charge; however, as described below, certain Services may be subject to payment.

- Registered members

The Website is intended to allow individuals interested in contributing to Cyberstand goals to participate in the development of those goals. In particular, by creating a registered account, users will be able to become actively involved in Cyberstand work, apply to the Cyberstand calls, participate to surveys.

- Newsletters and communications

The Trust-it will include members of Cyberstand within specific mailing lists, to ensure that those members are kept updated regarding important news and events related to the Website's scope, by sending out informative newsletters and other communications to registered users (unless they opt-out of this).

- Submission of applications

The Website also allows registered users to respond to different calls made by Cyberstand, including to apply to certain positions/functions within Cyberstand (namely, positions within Cyberstand Governance Bodies), to apply to become a host for upcoming Cyberstand events or to apply for grants awarded in connection with projects in which Cyberstand is involved.

- User support

Any questions concerning Cyberstand's activities in general can be addressed to Cyberstand via the General Enquiry Form, available at: /contact-us

Registered users can address questions specifically referring to the operation and use of the Website by writing an email to web@cyberstand.eu

- Events

Cyberstand may organise meetings for its community of registered users, which take place in different places around Europe and beyond, seeking to bring together a unique community of research data practitioners and industry and policy stakeholders to pursue the specific objectives of Cyberstand. Via the Website, registered users are able to sign-up to attend events and webinars for free or at a cost (paid via an external payment processor).

More information on Events is available at: /events

2. Copyright / Intellectual Property

Users of the Website may download or print copies of any and all materials on the Website for personal use. None of the information on this Website may be copied, distributed or transmitted in any way for commercial use without Trust-it written consent. For any materials downloaded from this Website, source and references must be acknowledged.

3. Liability

The material on this Website is provided for general information only. Trust-it makes no representations or warranties as to the accuracy or completeness of any materials and information incorporated thereto and contained on this website. Trust-it has a policy of continuous improvement of its communication and reserves the right to make improvements or changes to the online content without notice.

The use of the material (or any information incorporated thereto), in whole or in part, contained in this Website is the user's sole responsibility. Trust-it disclaims any liability for any damages whatsoever including, without limitation, direct, indirect, incidental and/or consequential damages resulting from access to the website and use of the materials provided therein.

Trust-it makes no representations about websites accessed through this Website which are not maintained, controlled or created by Trust-it. Trust-it does not endorse these sites and is not responsible for their content.

5.3 Cookie Policy

Cookies consist of portions of code installed in the browser that assist the owner in providing the service based on the purposes described. Some of the purposes of installing cookies may also require the consent of the user. When the installation of cookies takes place on the basis of consent, this consent can be revoked freely at any time following the instructions contained in this document.

Cookies are small text files that may be sent to and registered on your computer by the websites you visit, to then be re-sent to those same sites when you visit them again. It is thanks to these cookies that those websites can "remember" your actions and preferences (e.g., login data, language, font size, other display settings, etc.), so that you do not need to configure them again when you next visit the website, or when you change pages within a website.

Cookies are used for electronic authentication, monitoring of sessions and storage of information regarding your activities when accessing a website. They may also contain a unique ID code which

allows tracking of your browsing activities within a website, for statistical or advertising purposes. Some operations within a website may not be able to be performed without the use of cookies which, in certain cases, are technically necessary for operation of the website.

When browsing a website, you may also receive cookies from websites or web servers other than the website being visited (i.e., “third-party cookies”).

There are various types of cookies, depending on their characteristics and functions, which may be stored on your computer for different periods of time: “session cookies”, which are automatically deleted when you close your browser, and “persistent cookies”, which will remain on your device until their pre-set expiration period passes.

According to the law which may be applicable to you, your consent may not always be necessary for cookies to be used on a website. In particular, “technical cookies” – i.e. cookies which are only used to send messages through an electronic communications network, or which are needed to provide services you request – typically do not require this consent. This includes browsing or session cookies (used to allow users to login) and function cookies (used to remember choices made by a user when accessing the website, such as language or products selected for purchase).

- Types of cookies used by the Website

The Website uses the following types of cookies:

Browsing or session cookies, which are strictly necessary for the Website’s operation, and/or to allow you to use the Website’s content and Services.

Analytics cookies, which allow Trust-it to understand how users make use of the Website, and to track traffic to and from the Website.

Trust-it also uses third-party cookies – i.e. cookies from websites / web servers other than the Website, owned by third parties. These third parties will either act as independent data controllers from Trust-it regarding their own cookies (using the data they collect for their own purposes and under terms defined by them) or as data processors for Trust-it (processing personal data on Trust-it’s behalf).

For further information on how these third parties may use your information, please refer to their privacy policies:

Twitter

LinkedIn

- First-party cookies present on the Website

In detail, the cookies present on the Website are as follows:

Common

Technical name	Data Controller	Cookie type, function and purpose	Type of cookie	Duration
has_js	Trust-it	Functional cookie to remember whether a visitor has javascript in his browser	first party cookie/browsing cookie	Expires at the end of the session
consent_3rdparties_cookies	Trust-it	Cookie that records if the user accepted the 3rd parties cookies	first party cookie/browsing cookie	Expires at the end of the session
consent_additional_cookies	Trust-it	Cookie that records if the user accepted additional cookies	first party cookie/browsing cookie	Expires at the end of the session

Drupal

Technical name	Data Controller	Cookie type, function and purpose	Type of cookie	Duration
SSESSxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Trust-it	Drupal cookie that stores session identification.	first party cookie/session cookies	200000 seconds 200000 seconds - ~23 days
Drupal.tableDrag.showWeight	Trust-it	Drupal cookie that helps handle the consistent navigation of tabbed pages and forms across a range of different browsers.	first party cookie/functional cookies	1 Year

Google Analytics

Technical name	Data Controller	Cookie type, function and purpose	Type of cookie	Duration
_ga	Google	Google Analytics cookie used to distinguish users.	third party cookie/cookie analytics	2 Years
_gat _gat_gtag_UA_XXXXXXX_X	Google	Google Analytics cookie that does not store any user information; it's just used to limit the number of requests that have to be made to doubleclick.net	third party cookie/cookie analytics	60 seconds
_gid	Google	Google Analytics cookie used to distinguish users.	third party cookie/cookie analytics	24 hours

- Cookie settings

You can block or delete cookies used on the Website via your browser options. Your cookie preferences will be reset if different browsers are used to access the Website. For more information on how to set the preferences for cookies via your browser, please refer to the following instructions:

Chrome

Firefox

Internet Explorer

Safari

You may also provide set your preferences on third-party cookies by using online platforms such as AdChoice.

CAUTION If you block or delete technical and/or function cookies used by the Website, the Website may become impossible to browse, certain services or functions of the Website may become unavailable or other malfunctions may occur. In this case, you may have to modify or manually enter some information or preferences every time you visit the Website.

How can I express consent to the installation of Cookies?

In addition to what is indicated in this document, the User can manage the preferences for Cookies directly from within his browser and prevent - for example - that third parties can install them. Through the browser preferences it is also possible to delete the Cookies installed in the past, including the Cookie in which the consent to the installation of Cookies by this site is eventually saved. The User can find information on how to manage Cookies with some of the most popular

browsers such as the following addresses: [Google Chrome](#), [Mozilla Firefox](#), [Apple Safari](#) e [Microsoft Internet Explorer](#).

With reference to cookies installed by third parties, the User can also manage his own settings and revoke the consent by visiting the related opt out link (if available), using the tools described in the privacy policy of the third party or by contacting the same directly.

Without prejudice to the above, the User may use the information provided by [Your Online Choices](#) (UE), [Network Advertising Initiative](#) (USA) e [Digital Advertising Alliance](#) (USA), [DAAC](#) (Canada), [DDAI](#) (Japan) or other similar services. With these services it is possible to manage the tracking preferences of most advertising tools. The Data Controller therefore advises Users to use these resources in addition to the information provided in this document.