CCI4EU

Comprehensive Cancer Infrastructures 4 Europe

Deliverable number: D1.1

Deliverable title: Data Management Plan

Deliverable type	DMP — Data Management Plan
Deliverable responsible partner	TUD
Deliverable deadline	Month 6
Contractual date of delivery	Month 6
Actual date of delivery	Month 23
Dissemination level	PU - Public
Status of deliverable	Achieved 23 – updated version of the 18/03/25
Authors	Kai Gand (TUD), Jeannette Stark (TUD), Noémie Defourny (Sciensano), Nele Grapentin (DKG), Ellen Grießhammer (DKG)

Grant Agreement information table	
Grant Agreement number	101103746
Project acronym	CCI4EU
Project title	Comprehensive Cancer Infrastructures 4 Europe
Start date	1 May 2023
Duration	36 months
Project officer	Mr. Ioannis Vouldis

"This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No 101103746".

Change History

Version	Name	Activity	Date
First draft	Kai Gand (TUD)	Initial draft	22. August 2023
Version 1	Kai Gand, Jeannette Stark (TUD); Carla Finocchiaro (OECI); Nele Grapentin, Ellen Grießhammer (DKG); Noémie Defourny (Sciensano)	First full version & internal review	20. October 2023
Version 2 draft	Kai Gand (TUD)	Revised draft	01. March 2024
Version 2	Jeannette Stark (TUD); Carla Finocchiaro (OECI); Nele Grapentin, Ellen Grießhammer (DKG); Noémie Defourny (Sciensano)	Second full version & internal review	21. March 2024
Review of Version 2	Mr. Ioannis Vouldis + EU Review Committee	External review	Before 03. March 2024
Version 3 draft	Jeannette Stark (TUD)	revised draft after external review	10. March 2025
Version 3	Jeannette Stark (TUD); Carla Finocchiaro (OECI); Peggy Richter (TUD); Roxana Plesoianu (OECI); Claudia Valverde Morales (VHIO); Francesca Marangoni (ESO); Ellen Grießhammer (DKG)	Third full version & internal review	18. March 2025

Summary

The Data Management Plan (DMP) gives details about the data collected, processed, or generated by the project. As a basic principle, we will follow the FAIR principles to allow the smoothest data flow and accessibility as possible. All partners have been requested to contribute to the data summary. Overall, the project partners shall be sensitized and educated regarding the importance of the outlined data management tasks. The DMP compiles all relevant information in this regard. The document will act as a reference on the topic of data management to ensure the adoption of working principles that follow the presented precepts. Thus, the DMP is an umbrella document for aspects of the project related to data gathering, data flow, and data processing. An overview of these aspects and how to address the common FAIR principles is provided.

Table of Contents

Change History 2

Summary 2

1. Introduction 4

2. Fundamentals 4

3. Data Summary 5

4. FAIR data 11

4.1. Making data findable, including provisions for metadata 11

4.2. Making data accessible 12

4.3. Making data interoperable 12

4.4. Increase data re-use 13

5. Allocation of resources 13

6. Data security 15

7. Ethics 15

8. Risk assessment 15

9. Conclusions 15

Appendix 1: Key Concepts and Definitions for Consortium Members 17

Appendix 2: Methodology to Develop the Data Summary 20

Appendix 3: Risk Evaluation from DPO 24

1. Introduction

Effective research data management is a key priority in the CCI4EU project, ensuring that data is systematically collected, stored, processed, and shared in a manner that maximizes its long-term value and usability. As outlined in Part B of the project proposal, the Data Management Plan (DMP) is a critical component of this effort and has been developed within WP1/T1.3 by month 6 of the project timeline. A DMP serves as a framework for handling research data throughout the project lifecycle. It establishes clear strategies and procedures for data governance, security, documentation, and compliance with legal and ethical standards. By adopting a robust data management approach, CCI4EU aims to uphold data integrity, enhance collaboration among partners, and promote transparency and reproducibility of research findings. Moreover, a DMP facilitates the potential reuse of data beyond the project's duration, ensuring broader impact and accessibility.

This document is structured as follows:

- **Section 2** refers to fundamental principles and guidelines that ensure a shared understanding of key data management concepts within the project consortium.
- **Section 3** provides a comprehensive Data Summary, detailing the types of data collected, their sources, formats, and relevant Work Packages (WP), along with key considerations for data use at the WP level.
- **Section 4** explains how the project aligns with the FAIR (Findable, Accessible, Interoperable, Reusable) principles to optimize data usability and dissemination.
- **Section 5** presents additional, more granular aspects of data management, including repository structures, data preservation, and security protocols.

Through this structured approach, the CCI4EU project ensures that its research data is managed in a way that supports both immediate project needs and future scientific and policy advancements.

2. Fundamentals

This section provides an overview of the key principles and frameworks that inform the data management practices within CCI4EU. These guidelines ensure a shared understanding among consortium members regarding data governance, security, and compliance requirements. The specific definitions, legal references, and technical explanations of these concepts are compiled in the appendix to serve as a practical reference for project partners. The data management strategy of CCI4EU aligns with well-established European and international frameworks, including:

- **The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)** – the foundational legal framework for data protection in the European Union, governing the processing, storage, and transfer of personal data.
- **The European Data Protection Supervisor (EDPS) Guidelines** – outlining best practices for compliance with data protection regulations within EU-funded research projects.

- **The FAIR Data Principles** – ensuring that research data is **Findable, Accessible, Interoperable, and Reusable** to maximize its usability beyond the duration of the project.
- **The Horizon Europe Open Science Guidelines** – promoting data accessibility, transparency, and responsible data sharing within EU research programs.
- **The E-Privacy Directive (2009/136/EC)** – addressing confidentiality in electronic communications and further strengthening the GDPR principles regarding digital privacy.
- **Best practices in Research Data Management (RDM)** – incorporating principles from organizations such as the European Open Science Cloud (EOSC) and the Research Data Alliance (RDA) to enhance data security and usability.

These frameworks collectively provide the foundation for how data is handled, shared, and protected within the CCI4EU project. Further details on key concepts such as data protection principles, data subject rights, accountability, confidentiality, and legal requirements for processing and transferring data can be found in **Appendix 1**, where specific terms and definitions are outlined in greater detail for the project consortium.

3. Data Summary

The CCI4EU project collects and generates various types of data to support its objectives:

- **Project management data and internal communication data** are collected and processed to facilitate efficient project coordination and collaboration among partners.
- **Communication channel data and personal data** include information related to website usage, e-mail communication, and participant details.
- **Research and dissemination data** encompass reports, position papers, survey results, and outreach studies that contribute to the scientific and policy-related outcomes of the project.
- **Service-related data** include technical logs, API interactions, and benchmarking records from the Maturity Model Webtool and LimeSurvey assessments.
- **Capacity building and training data** consist of materials, evaluations, and participant records from educational and training activities.
- **Deep Dive and capacity building intervention data** capture assessments and reports related to the targeted interventions within the project.
- **Administrative and financial data** are used for financial management, reporting, and compliance with funding requirements.
- **Metadata and documentation data** provide structured descriptions of datasets, ensuring accessibility and reusability.

An explanation of the methodology used to derive the data summary, including data collection, processing, and classification approaches, is provided in **Appendix 2**. In the following, we provide a breakdown of data categories used in the CCI4EU project, their sources, formats, and associated Work Packages (WPs).

Data Category	**Project Management Data**
Data Type	Textual (internal documents, reports, meeting minutes, technical specifications, deliverables)
Source	Project partners, WP leaders
Format	DOCX, PDF, PPTX, XLSX, CSV
Size	< 1 G
Purpose	Coordinating and managing the project
GDPR Issues	No personal data included
WP	All WPs
Data Management Strategy	Stored on SharePoint with access restricted to project partners. Retained in accordance with project and institutional policies, ensuring long-term accessibility where required. Access control, HTTPS encryption, and versioning enabled for document integrity and security.

Data Category	**Internal Communication Data**
Data Type	Textual, Multimedia (mailing lists details, chat logs, authentication data, meeting recordings)
Source	Project partners, WP leaders
Format	TXT, CSV, XLSX, PDF
Size	< 1 G
Purpose	Facilitating internal communication and collaboration within the project
GDPR Issues	As this data contains sensitive information, access is restricted to project members only. The project coordinator is responsible for the secure storage of the project management data.
WP	All WPs
Data Management Strategy	Stored on SharePoint and internal communication platforms (e.g., Microsoft Teams, e-mail servers)**.** Access is restricted to project members **only**. Meeting recordings are temporarily stored for transcription purposes and deleted thereafter. Data is protected via access controls, encryption, and secure authentication methods.

Data Category	**Communication Channel Data**
Data Type	Structured, Log Data (page views, visits, hits, countries number of visitors by country)
Source	Website visitors, newsletter subscribers
Format	CVS
Size	< 1 G
Purpose	Community building, communication, advocacy, and user tracking
GDPR Issues	The CCI4EU website does not collect or process personal data and complies with Article 25 of the GDPR (data protection by design and by default). No personally identifiable log data is stored or processed. A cookie and privacy policy has been implemented and reviewed to ensure full compliance with EU

	data protection regulations. The website is managed by Healthropy, a spin-off of the University of Genoa, which was selected as a subcontractor after evaluating three offers.
WP	WP8
Data Management Strategy	Website analytics data (page views, visits, hits, and country-based visitor counts) is stored on secure servers with GDPR-compliant consent mechanisms. Email addresses for newsletters and press contacts are securely stored and used exclusively for project-related communication. No third-party tracking services are used beyond what is necessary for basic analytics. Users are informed about data collection, storage, and usage policies via the cookie consent banner and privacy policy. Any future modifications to website policies are publicly documented at cci4eu.eu/policy.

Data Category	**Personal Data**
Data Type	Personal (sociodemographic data (first name, surname, institutional e-mail addresses, profession))
Source	Representatives responding on behalf of the CCIs
Format	CVS, XLSX, PDF
Size	< 1 G
Purpose	Facilitating self-assessment and Deep Dive activities, enabling coordination and follow-ups with CCI representatives.
GDPR Issues	Informed consent is collected from participants
WP	WP2, WP3, WP6
Data Management Strategy	Personal data is collected with informed consent for the self-assessment. Only first name, surname, institutional e-mail address, and profession are collected. • Self-assessment (WP2, WP3): In T0**,** data collection was conducted via LimeSurvey, while in T1, data collection takes place via the Maturity Model Webtool**.** Exports from LimeSurvey are encrypted and stored in a password-protected SharePoint folder with restricted access (WP3 members only). In T1, informed consent will be obtained directly through the Maturity Model Webtool before data submission. • Deep Dives (WP6): Data is collected and stored in XLSX format within restricted-access project repositories. Access is granted only to authorized WP6 members involved in Deep Dive activities. Data is retained only for the duration of the project and will be deleted after project completion unless further retention is required for follow-up studies.

Data Category	**Research & Dissemination Data**
Data Type	Textual, Analytical (reports, position papers, survey analysis, dissemination & outreach studies)
Source	Data collected from project activities, stakeholder engagement, research output, and previous Joint Actions such as iPAAC and JA CRANE.
Format	CSV, RTF, XLSX, PPTX, PDF, DOCX, ODT, JPEG/JPG
Size	< 3 G
Purpose:	Collecting and analyzing research findings
GDPR Issues	Best practices for protecting participant data in user research will be followed.[1]
WP	All WPs
Data Management Strategy	Research and dissemination data is stored securely on SharePoint for internal collaboration and publicly shared on Zenodo or other open-access repositories where applicable. Data is version-controlled to ensure integrity. Stakeholder input and research outputs are documented systematically. Sensitive data is anonymized where necessary before publication. Access to unpublished research data is restricted to project members until dissemination.

Data Category	**Service-Related Data**
Data Type	Log Data, Structured (Webtool usage data, API logs, error logs)
Source	LimeSurvey, Maturity Model Webtool, CCIs
Format	JSON, CSV, XML
Size	< 1 G
Data Collection Purposes	Monitoring tool usage, ensuring proper functionality of the Webtool and LimeSurvey
GDPR Issues	The Maturity Model Webtool and LimeSurvey store session cookies necessary for authentication and security purposes. **Maturity Model Webtool:** Stores predefined login credentials (not personalized) and device information (IP address, operating system, browser name). No optional tracking cookies are used. Users are informed about data storage when credentials are issued. Additionally, the Webtool allows storing names of CCI contact persons, which are addressed in the data category Personal Data. Participants have the right to withdraw consent, request deletion, or access their data. **LimeSurvey:** No additional tracking beyond authentication logs occurs. LimeSurvey data is stored on password-protected servers within the EU and is

[1] See for example: https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf

	only accessible to designated WP2 and WP3 members**.** Participants have the right to withdraw consent, request deletion, or access their data.
WP	WP2, WP3
Data Management Strategy	Service-related data is stored securely on designated servers with restricted access. Webtool and LimeSurvey logs are monitored for performance analysis and error tracking. No additional tracking cookies are used. Webtool data is stored within secure databases with controlled access, and LimeSurvey data is retained on password-protected servers hosted by TUD Dresden. Only authorized WP2 and WP3 members have access to relevant data. Data retention follows project guidelines, and logs are deleted after the necessary period for debugging and analysis. The Web Tool has different access levels for various stakeholders (e.g., Administrators and Project Leaders, Deep Dive Experts, and CCI access).

Data Category	**Capacity Building & Training Data**
Data Type	Training materials, evaluation forms, participant data for online courses and regional conferences
Source	ESO (European School of Oncology) and e-ESO platform, WP4 & WP5 participants, structured expert interviews, literature reviews, stakeholder feedback
Format	PDF, MP4, XLSX, SRT, CSV, LMS exports,
Size	< 170 G
Data Collection Purposes	Providing capacity-building resources and training to CCIs across Europe; Tracking learning activities (engagement, course completion, evaluation)
GDPR Issues	Participant data is collected following GDPR regulations; evaluation forms are anonymized.
WP	WP4, WP5
Data Management Strategy	Training materials and recorded sessions are stored securely on the e-ESO platform, the CCI4EU digital platform, and internal repositories. Evaluation forms are collected in CSV format and anonymized before analysis. Metadata tagging (e.g., 'CCI4EU') is applied for structured searchability. Access levels are defined for participants, administrators, and content managers. Learning activities (e.g., course participation, completion rates) are tracked for evaluation. Selected materials remain accessible beyond the project duration, with participation certificates issued where applicable. Data protection measures, including encryption and controlled authentication, ensure secure handling and storage.

Data Category	**Deep Dive & Intervention Data**
Data Type	Reports, assessments, intervention tracking data, situational analysis reports
Source	Deep Dive teams, WP6 participants, CCI representatives
Format	DOCX, PDF, XLSX
Size	< 5 GB
Data Collection Purposes	Evaluating Deep Dive interventions and their impact on CCIs
GDPR Issues	Personal data (first name, surname, institutional e-mail address, profession) is collected to facilitate Deep Dive activities and is detailed in the Personal Data category.
WP	WP6
Data Management Strategy	Data collected from Deep Dive interventions is stored securely on the SharePoint. Reports and assessments are structured and categorized for streamlined retrieval. Intervention tracking data is regularly updated and archived for long-term impact analysis. Aggregated data is used for reporting and evaluation, ensuring no personal identifiers are included in public outputs. Data retention follows project guidelines, with periodic reviews to determine continued relevance and deletion timelines.

Data Category	**Administrative and Financial Data**
Data Type	Budget reports, funding documentation, financial transactions, contracts
Source	Project partners, WP leads, funding agencies
Format	SLSX, PDF, CSV
Size	< 1 G
Data Collection Purposes	Managing project funding, financial reporting, and compliance
GDPR Issues	Contracts may contain personal data (e.g., names, contact details); access to financial data is restricted to project coordinators and authorized personnel.
WP	WP1
Data Management Strategy	Contracts may contain personal data (e.g., names, contact details), which is processed in compliance with GDPR regulations. Access to financial data is strictly restricted to designated personnel. Any shared financial summaries are anonymized to exclude personal information where possible.

4. FAIR data

In Table 1, we summarise first basic provisions how to address the EC FAIR principles. Further details follow in the subsequent sub-chapters.

Table 1: EC FAIR principle - basic provisions

Findable	Results in the form of public deliverables are published on the project website. The reciprocal transfer of information between the partners will be in accordance with GDPR requirements.
Accessible	Summary reports on the criteria included in CCI MM (WP2), from the country database related to the CCI4EU survey (WP3), the educational courses delivered via the e-ESO platform (WP5) destined at first to registered users and then to everybody by re-publishing as open access material, reports on Deep Dives (WP6), the assessment of CB achievements (WP7) will be accessible – at least as summary reports, the provision of detail reports varies from case to case (given the sensitivity of the data or the relevance of single data points as overall assessments are in focus).
Interoperable	All data from WPs will use a formal, accessible, shared, and broadly applicable language for knowledge representation. Specifically, for educational videos and slides (WP5) they will be available by contacting the ESO IT team which will provide the MP4 and PDF files.
Reusable	CCI4EU will make available cleaned, de-identified copies of the final data set used in conducting the final analyses and the report on the results generated by the project for use in further collaborative studies.

4.1. Making data findable, including provisions for metadata

Ensuring the findability of research data is a fundamental aspect of the FAIR principles. In the CCI4EU project, various strategies are implemented to guarantee that datasets are easily discoverable and identifiable by both humans and machines. To achieve this, relevant datasets generated within CCI4EU will be assigned Persistent Identifiers (PIDs), such as Digital Object Identifiers (DOIs) or other recognized standard identifiers. These PIDs provide a stable reference, ensuring that datasets remain accessible and citable over time. Furthermore, metadata will be structured according to internationally recognized standards such as Dublin Core, DataCite Metadata Schema, and ISO 11179. The metadata will include key descriptive elements such as the dataset title, author information, keywords, project references, data creation details, licensing information, and links to related datasets or publications. To enhance discoverability, datasets will be registered in open data repositories and indexed in relevant data catalogs such as Zenodo, integrating data into the European Open Science Cloud (EOSC) where applicable, and ensuring visibility in broader research infrastructures such as OpenAIRE.

Another aspect of findability is the use of clear naming conventions and version control. Each dataset will be systematically named following a predefined format, and version numbers will be assigned to track modifications and updates. Older versions of datasets will be archived to maintain referenceability, ensuring that no information is lost over time. Additionally, within the CCI4EU project, datasets will be identified and coded based on specific countries and, if necessary, further categorized by regions. To further strengthen data findability and ensure alignment with existing research efforts, CCI4EU integrates insights and data references from previous Joint Actions such as iPAAC and JA CRANE. CCI4EU ensures that these data sources are properly referenced in metadata documentation, facilitating traceability and enabling future research initiatives to build upon existing knowledge.

Since the data analysis will be limited to the scope of the CCI4EU project, broad discoverability outside of this context will not be facilitated. Instead, key findings will be made available in summative reports, ensuring that the project outcomes remain accessible. The publication of individual datasets is not deemed relevant for public access, as they may contain sensitive information affecting the legitimate interests of cancer care institutions. The primary focus is on analyzing cancer care structures as a whole, rather than on individual datasets.

4.2. Making data accessible

The CCI4EU project follows the European Union's Open Science policy, adhering to the principle of sharing research outputs as openly as possible while ensuring necessary safeguards for sensitive data. To maximize accessibility, peer-reviewed publications resulting from the project will be made freely available through gold or green Open Access. To further facilitate access, links to these publications will be provided on the project website and deposited in Zenodo, ensuring long-term availability. Educational materials developed within the project, including those delivered via the e-ESO platform, will also be republished as open-access resources whenever possible. While open access is prioritized, not all project data will be publicly available. Some datasets contain sensitive information related to healthcare policies in EU Member States, which are typically not openly accessible. In such cases, only summarized results will be shared to provide an overview of the socioeconomic status, healthcare systems, and research funding landscapes analyzed in CCI4EU. No embargo on publications or data is foreseen within the project, ensuring timely dissemination of results.

For long-term preservation and dissemination, Zenodo has been chosen as the primary repository for storing project research outputs. Zenodo provides persistent identifiers (DOIs), making it a reliable platform for ensuring visibility of research findings. As part of the OpenAIRE initiative, Zenodo is widely used for European Commission-funded research projects and does not require special access arrangements.

4.3. Making data interoperable

To facilitate seamless data exchange and integration across different systems, the CCI4EU project ensures that datasets are structured according to widely accepted metadata and documentation standards. This approach enhances interoperability and enables researchers, policymakers, and stakeholders to efficiently reuse and combine data for further analysis. Generated datasets, if relevant, will be preserved and annotated

with essential metadata, ensuring that they remain understandable and usable across different platforms. The metadata will include:

- **General Information:** Dataset title, dataset identifier, responsible partner, author information, date of data collection, project title, and funding sources.
- **Sharing and Access Information:** License/access restrictions, repository links, and references to derived data sources.
- **Dataset and File Overview:** Description of sub-datasets, status of data documentation, and plans for future updates.
- **Methodological Information:** Data collection methods, software and tools used, and relevant environmental or experimental conditions.

To promote interoperability, the CCI Maturity Model Webtool and in the beginning for T0 assessment LimeSurvey platform will be used as structured data formats. These platforms ensure that the data collected through assessments and surveys is standardized, making it easier to integrate with existing research frameworks and policy tools. Data will be gathered from multiple EU Member States and select Associated Countries. WP2 and WP3 collaborate to design relevant survey questions, aligning with key themes such as cancer care structures, research integration, clinical research, patient pathways, and screening programs.

4.4. Increase data re-use

To ensure data reusability, all authors of deliverables and internal documents are encouraged to document their methodology, data collection processes, selection criteria, and analysis procedures. This commitment to scientific rigor and transparency enhances the meaningful reuse of data and supports evidence-based decision-making in cancer care infrastructures. While not all data will be made publicly available, **summarized reports**—such as D3.1 on the status quo of cancer infrastructures—will provide a comprehensive overview. These summaries ensure that key findings remain accessible and valuable for future research and policy development. Additionally, subsequent Joint Actions can leverage this data to implement measures addressing identified weaknesses in cancer care systems.

Quality assurance processes follow the principles of validity, reliability, and objectivity. Experienced researchers with strong methodological expertise conduct data collection and evaluation. Measures to prevent data manipulation include technical protections (e.g., password protection, firewalls) and safeguards against data loss, such as regular backups and version control mechanisms in SharePoint. Furthermore, raw survey data undergoes cross-validation checks to verify consistency among respondents and CCIs within different Member States and Associated Countries.

5. Allocation of resources

No additional costs will occur linked to all the measures and the approach within the present document. Allowing this kind of work mode was included in the project calculation from the very beginning and is, given the longstanding experience of the project partners, no additional work effort. There are also no

immediate costs anticipated to make the datasets produced FAIR. These efforts are already included in the staff costs (except for possible open-access fees issued by scientific journals). The datasets will be deposited in the Zenodo repository for at least 5 years after the conclusion of the project. The use of Zenodo is free of charge up to 2 GB per dataset. Any unforeseen costs related to open access to research data would however be eligible for reimbursement during the duration of the project under the conditions defined in the GA.

In principle, each partner should respect the policies set out in this DMP. Datasets have to be created, managed and stored appropriately and in line with the EC and local legislation. In principle, all partners are responsible for data generation, metadata production and data quality. The principal investigator of each partner will have overall responsibility for implementing the DMP. Specific responsibilities are to be assigned depending on the data and the internal organization in the WPs and tasks where data is created. It needs to be ensured that only necessary data accesses are taking place. The primary investigators are in particular:

- The lead of WP1, the project coordination, takes the roles of overall management also with regard to ensuring the provisions on data management in general given by the present DMP.
- For WP2 data management: Dr. Ellen Grießhammer (DKG, WP-Leader of WP2), Eva Jolly (KI, WP-Leader of WP2), Dr. Peggy Richter (TUD, Task-leader WP2, task 2.3.)
- For WP3 data management: Sciensano as WP-lead: Dr. Marc Van Den Bulcke, Dr. Régine Kiasuwa Mbengi, Dr. Noémie Defourny
- For WP6 data management: Willien Westerhuis, Simon Oberst

Nevertheless, all project participants shall be sensitized and educated regarding the importance of outlined data management tasks. The current DMP builds the baseline to do so. The DMP acts as a reference on the topic of data management to ensure the adoption of working principles that follow the presented precepts. The compulsiveness of the precepts given by the DMP, especially the FAIR principles, when it comes to data-related processes has been underlined by the project and its management bodies.

Additionally, the project's Data Protection Officer (DPO) is responsible for overseeing compliance with GDPR and other data protection regulations. The DPO ensures that all personal data processing within the project adheres to legal requirements and supports project partners in implementing necessary safeguards:

- **Data Protection Officer (DPO):** Norbert Maggi, norbert@ieee.org

The coordinator of the project has created a *Microsoft SharePoint (Microsoft OneDrive solution)*[2] to host the project's internal data and as an internal project repository. This includes project deliverables, document drafts, Word and PowerPoint templates to ensure a uniform (external) presentation of the project, presentations from project meetings, or grant data like the Grant Agreement. The overall objective is to support the effective and efficient joint work of the project consortium members. This is why there should be centralised storage of all relevant material so that everyone knows where to look for needed information

[2] See: https://www.microsoft.com/en-us/microsoft-365/sharepoint/collaboration

and documents. Also, SharePoint allows collaborative, simultaneous editing of typical Office documents both directly in the Internet browser and through the Office application. This ensures that documents do not have different, possibly conflicting version statuses. Uniformity and correctness of data and documents are, thus, ensured. Furthermore, the SharePoint folders can be accessed by invitation only (initially given to the active project consortium members) and with an access token every time requested when logging in. More detailed or fine-grained access restrictions are possible. Rightful access is ensured through secure passwords. Data transfer is secured via HTTPS protocol. This already provides a good level of protection. Given the above features and benefits, the coordinator chose SharePoint as the internal project repository.

6. Data security

Backup of data is conducted using secure backup systems. For these purposes, each institution provides a secure and fail-safe IT infrastructure. Particular data backup and threat monitoring measures are in place.

7. Ethics

No sensitive/special personal category of data (§9 GDPR) will be collected in the course of the project. Primarily, professionals will report on their collective assessment of particular aspects of the state of cancer care in Europe but not on the situation of particular individuals, etc. Thus, several safeguard mechanisms as per GDPR are not necessarily implemented. Ethical approval is also not needed, given the mode of assessment.

8. Risk assessment

No sensitive, health-related personal data is collected as part of the project. However, as part of the survey to determine the maturity of (potential) CCIs, at least *personal data in the sense of contact information* of members/employees of these (potential) CCIs or the entities behind them is collected. This appears necessary for the targeted recruitment of participants. However, the depth of intrusiveness with this form of data collection remains low. It only involves contact/context data of survey participants, some of which is publicly available anyway, in order to be able to address them personally or in a reasonably targeted manner. The survey participants should then reflect a purely professional reporting perspective in the survey. The basis of the data collection is the informed consent in the survey (§ 13 GDPR) with all the necessary mechanisms of the GDPR, laid down in the data protection declaration of the survey.
Nevertheless, in order to uncover any potential risks that may not be immediately apparent in this form of data collection, we have carried out a comprehensive analysis. This risk assessment can be found in Appendix 3. Overall, this results in only a low-impact assessment.

9. Conclusions

The current DMP provides a summary of all data-related aspects of the project. Respective overviews are provided to make clear how the project is intended to work and process data on a generic level. Technical/operational details are provided in the particular project deliverables. All this is related to data as one of the most crucial immaterial resources. Thus, it is important to sensitise the whole consortium for

the importance and attentiveness of data gathering and processing. The DMP provides the basis to have all this fully considered. The FAIR principles support the aspiration of having free and openly accessibly data as much as possible but, at the same time, restrictions when accessing data as much as needed. The further aim of the DMP and Task 1.3 is to support all upcoming considerations when data gathering and processing is touched and always provide respective guidance to the project partners. Further on, we will comply with the Grant Agreement (cf. Annex 5, Article 17) obligations to update the DMP by updating the document internally using SharePoint to incorporate any changes or additions to the items listed here. In this way, the DMP as a whole will always remain up to date. If necessary, the changes can also be particularly reported in order to highlight important differences and to make it clear to everyone what is now to be paid particular attention to.

Appendix 1: Key Concepts and Definitions for Consortium Members

This appendix provides detailed explanations of key data management concepts, legal frameworks, and principles referenced throughout this document. It serves as an internal resource for consortium members to ensure consistent understanding and compliance with best practices in research data management.

1. Legal and Regulatory Frameworks

General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)

The GDPR is the primary legal framework governing data protection in the European Union. It establishes rules for the collection, storage, processing, and transfer of personal data to protect individuals' rights and privacy. Key principles include:

- **Lawfulness, fairness, and transparency** – Data must be processed lawfully, fairly, and in a transparent manner.
- **Purpose limitation** – Data must be collected for specified, explicit, and legitimate purposes.
- **Data minimization** – Data collected should be limited to what is necessary for the intended purpose.
- **Accuracy** – Data must be kept accurate and up to date.
- **Storage limitation** – Data should be stored for no longer than necessary.
- **Integrity and confidentiality** – Data must be processed securely to protect against unauthorized access, loss, or destruction.

European Data Protection Supervisor (EDPS) Guidelines

The EDPS provides guidance on GDPR compliance, particularly for EU-funded research projects. It emphasizes data subject rights, accountability, and transparency in data processing.

FAIR Data Principles

The FAIR principles ensure that research data is **Findable, Accessible, Interoperable, and Reusable**:

- **Findable** – Data should be assigned a persistent identifier and documented with metadata.
- **Accessible** – Data should be stored in a format that allows authorized users to access it easily.
- **Interoperable** – Data should be formatted for integration with other datasets and systems.
- **Reusable** – Data should be clearly licensed and documented for future use.

Horizon Europe Open Science Guidelines

Horizon Europe promotes open science by requiring research projects to share data openly when possible. It emphasizes transparency, reproducibility, and responsible data sharing.

2. Key Data Protection Concepts

Accountability (Article 5(2) GDPR): Organizations processing personal data must demonstrate compliance with GDPR principles through documentation, security measures, and internal policies.

Confidentiality and Data Security: Confidentiality requires that personal data is accessible only to authorized personnel. Security measures such as encryption, access controls, and secure storage must be implemented to prevent unauthorized access.

Consent (Article 4(11) GDPR): Consent must be freely given, specific, informed, and unambiguous. Data subjects have the right to withdraw consent at any time.

Data Subject Rights (Chapter III GDPR): Individuals have several rights regarding their personal data, including:

- **Right of access** – To obtain confirmation of data processing and access to their data.
- **Right to rectification** – To correct inaccurate or incomplete data.
- **Right to erasure ('right to be forgotten')** – To request deletion of their data under certain conditions.
- **Right to restriction of processing** – To limit how data is processed.
- **Right to data portability** – To receive data in a structured, commonly used format.
- **Right to object** – To oppose data processing for certain purposes.

Data Minimization (Article 5(1)(c) GDPR): Data collection should be limited to what is necessary for a specific purpose. Unnecessary or excessive data should not be collected or retained.

Data Protection Impact Assessment (DPIA, Article 35 GDPR): A DPIA is required when processing activities pose a high risk to individuals' rights and freedoms. It assesses potential risks and outlines measures to mitigate them.

Data Breaches and Incident Response (Article 4(12) GDPR): A personal data breach is a security incident that leads to unauthorized access, disclosure, or loss of personal data. Organizations must report breaches to the relevant authorities within 72 hours if there is a risk to individuals' rights.

3. Roles in Data Processing

Data Controller (Article 4(7) GDPR): The data controller determines the purposes and means of processing personal data. The controller is responsible for ensuring compliance with GDPR requirements.

Data Processor (Article 4(8) GDPR): A data processor processes personal data on behalf of the data controller. Processors must follow the controller's instructions and implement security measures.

Data Protection Officer (DPO, Article 37 GDPR): The DPO is responsible for overseeing GDPR compliance, advising the organization on data protection issues, and acting as a contact point for data subjects and authorities.

4. Data Anonymization and Pseudonymization

Anonymization (Recital 26 GDPR): Anonymized data can no longer be linked to an individual and is no longer subject to GDPR regulations. Effective anonymization requires removing or altering identifiers permanently.

Pseudonymization (Article 4(5) GDPR): Pseudonymization replaces identifiable information with coded references. While pseudonymized data remains subject to GDPR, it reduces privacy risks by separating identity from the dataset.

5. Ethical Considerations in Data Management

The CCI4EU project follows ethical guidelines to ensure responsible data handling:

- **Explicit prior informed consent** – No data is collected without the individual's consent.
- **Limited data use** – Data is processed only for project-related purposes.
- **Data minimization** – Only necessary data is collected.
- **Confidentiality safeguards** – Employees and participants' identities are protected.
- **Compliance with informed consents** – Data is processed within the limits of agreed-upon consent terms.

6. Data Transfers and Storage

Data Transfers Outside the EU (Chapter V GDPR): Data transfers to countries outside the EU/EEA must be protected through:

- **Adequacy decisions** – The recipient country ensures adequate data protection.
- **Standard contractual clauses (SCCs)** – Legally binding agreements between sender and recipient.
- **Binding corporate rules (BCRs)** – Internal rules for multinational companies ensuring GDPR compliance.

Data Storage and Security Measures: Data in CCI4EU is stored on secure servers with restricted access. Security measures include:

- **Encryption** – Protecting sensitive data from unauthorized access.
- **Access controls** – Limiting access to authorized users.
- **Regular audits** – Ensuring compliance with security policies.

Appendix 2: Methodology to Develop the Data Summary

Overview of the data collection or processing activities

To get a general overview of the data collection or processing activities within the project, we used the specifications given in the DoA as a first basis to get a first *overview of the aspects relevant to the DMP*. Accordingly, we examined the DoA for elements that relate to an activity in the direction of data collection or processing and systematically compiled them per WP. Furthermore, we designed an *internal assessment form* to get further information of the consortium members using Google Forms[3] sheet. With this, we requested contact and organisation details of responsible persons for inquiries on the DMP or research data management in general and an assessment of the proposed overview of data collection or processing activities. This has been spread to the whole consortium (both with a respective announcement during the project kick-off meeting on 23 May 2023 and afterward via e-mail). With 27 responses, including representatives from all WP leads, we got sufficient insights and expertise from the consortium. As a result of the above-mentioned document analysis on a general overview of the data collection or processing activities, we derived Figure 1 to show the data-related interrelations of the WPs. Table 2 provides more details on this.

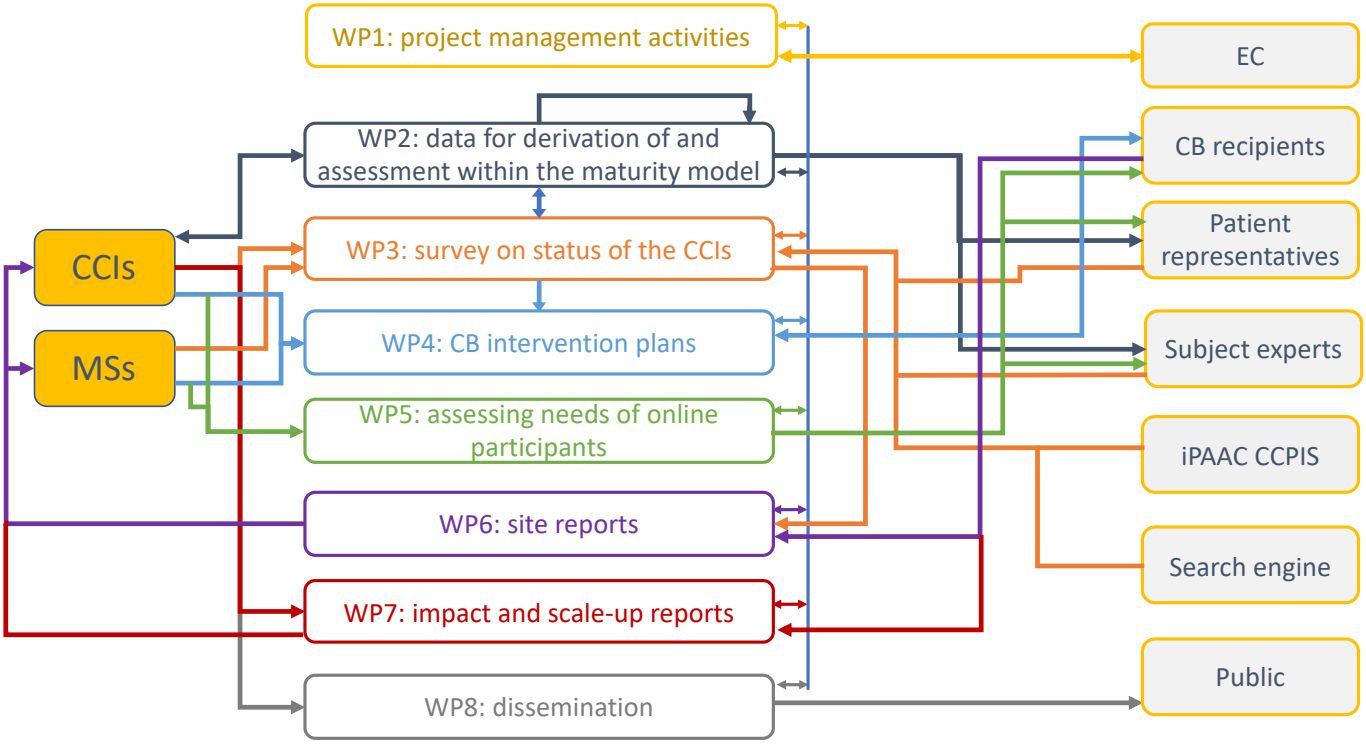

Figure 1: Overview of the data collection or processing activities as per DoA - WP interrelations

The overview shows the multitude of relations of the WPs with regard to data in general. Also, the basic relations to entities from out of the project consortium (left CCIs and MSs as major objects of study; data sources and partners/collaborators on the right). Almost all WPs are interrelated with each other (as

[3] See: https://docs.google.com/forms

indicated by the blue vertical connection line in the middle), as to be expected, given the comprehensive project approach. Double-sided arrows show data input and output/backflow relations. Single-sided arrows indicate single input/output relations only. As introduced here, the analysis helps to better overview the data-related aspects.

Table 2: Details on WP data collection or processing activities as per DoA

WP	Data collection or processing activities as per DoA	Connection/data collection from
WP1	Deriving/overviewing the derivation of deliverables	all WPs
	Gather input data and assemble these for reports, deliverables, forms, etc. to the EC as part of the regular project execution and monitoring	all WPs
	Provide reports, deliverables, forms, etc. to the EC as part of the regular project execution and monitoring	EC
	Coordinative communication between WP leaders and task members	all WPs
	Collect financial data and spread funds	all WPs
	Gather and distribute minutes of project meetings/boards	all WPs
WP2	Coordination with other WPs and subjects' experts through an adapted Delphi Process for agreement of proposed criteria	other WPs Subject experts
	Define criteria including Quality Indicators, defined and agreed upon with all members of WP2	WP2
	Collection of data from CCIs and for the assessment and description of a CCI's maturity level. This data will be collected using a web-tool.	CCIs
WP3	Collecting structured information and data from EU MSs and associated countries on the functioning and organization of cancer research and its integration with cancer care, and the presence and level of maturity of already existing CCIs: quantitative survey results	MSs
	Reuse results from the iPAAC Cancer Control Policy Interview Survey (CCPIS)	iPAAC CCPIS
	Reuse results from the JA CRANE, survey performed in WP7	JA CRANE WP7
	Use themes and criteria of the CCI MM developed within WP2	WP2
	Analyse the results in the CCI MM, cluster the CCIs according to type, size and level of maturity, and choose a putative list of CCIs for Deep Dive intervention in WP6	WP6
	Identification of the needs of EU CCIs in terms of building capacity for cancer research and integration in cancer care	CCIs
	Search using key words will be performed to identify the information already collected about cancer research and its integration in the care	Search engines like Embase, Pubmed, tripdb databases
	Country-specific summaries drafted and validated by MS representatives	MSs
	Deployment of online CCI4EU survey, based on the list of themes and criteria developed by the WP2 and complemented with contextual features	WP2 Subject experts
	Virtual meetings with relevant informants and/or MS representatives will be organized to gather qualitative data on CCIs at the relevant level of organisation for each theme (i.e. nation, region, hospital network, etc), where necessary due to lack of information in tasks 3.1 and 3.2.	MSs, CCIs Subject experts

	On-site visits with relevant informants and/or MS representatives will be organized to gather qualitative data on CCIs at the relevant level of organisation for each theme, where necessary due to lack of information in the tasks 3.1 and 3.2.	MSs, CCIs
	Collect feedback from European network of cancer patient organizations through ECPC or covered by the survey depending on the informant profiles	Patient representatives
	Assessment data: CCIs by region and/or nation will be clustered according to their level of maturity and as regards the criteria	CCIs
	Putative list of CCIs which would benefit from specific deep dive interventions in WP6 will be drawn up, together with the themes requiring most targeted CB interventions	CCIs WP6
	Readiness of implementing changes of the countries will be assessed (foreseen through the online survey)	MSs
	For the survey purposes, personal data from the survey participants will be collected and used recruit survey participants from (potential) CCIs in a targeted manner. This includes the first and last name, address, e-mail address, phone number (if known), and, as a rule, the IP address. Still, this relates only to their professional roles as members/employees of (potential) CCIs and to their assessment of the cancer care/research in the relevant setting they are capable of providing information.	CCIs
WP4	Assessing CB-related needs of each CCI in a MSs or an individual region within a MS	CCIs MSs
	Success assessment of the programme by assessing the CB recipients' degree to have assimilated lessons learnt and show readiness to implement the interventions of such a programme	CB recipients
	Offer CB general menu	CB recipients
	Interventions assess and include individual, institutional and system perspectives as well as the patients' insights in the development of personalised CB tailored interventions	Subject experts Patient representatives CB recipients
	Identified CCIs from Task 3.3 will be contacted and a more focused CB plan will be tailored together with the CCI: derive discussion minutes	CCIs WP3
	Provide basket of specific interventions as CB to all MSs and CCIs using online platforms for training and F2F	MSs CCIs
	Report on analysing the local systems capacity and prerequisites for receiving support and implement improvements	MSs CCIs
WP5	Reuse ESO's digital learning platform (e-ESO) for access by trainers and trainees from all MS' CCIs' (participant data; Online learning material, organized as online seminars, online courses, online case discussions, with the possibility of direct interaction between trainers and trainee)	MSs CCI
	Define/set up resource centre to compile/organize resources that may be used by CB implementers, including trainers and trainees, to plan and implement their interventions (resources and interventions connected to the dimensions fulfilled to meet CCI maturity criteria)	CB recipients
	Providing coaching/orientation programme for the expert trainers including expert patients	Patient representatives Subject experts
WP6	Situational analysis reports (of CB interventions)	CB recipients CCIs MSs

	Final reports post intervention (of CB interventions)	CB recipients	CCIs	MSs
	Final reports for each Deep Dive site	CB recipients	CCIs	MSs
	Assessment of the methodology of the interventions to be used	CB recipients	CCIs	MSs
	Conference evaluation report	CB recipients	CCIs	MSs
WP7	Final report of the impact of CB interventions in each site and across the EU MSs	CB recipients	MSs	
	CB outcome reports	CB recipients		
	Derivation of recommendations on how to structure future capacity building projects and how to develop and grow CCIs in different contexts	CCIs	MSs	
	Document and recommend potential funding mechanisms for CCIs	CCIs		
	Overall report of the CB actions and recommendations for future CB projects	CB recipients		
WP8	Compile and provide: Dissemination, Communication and Exploitation Plan (DEC-Plan)	Public		
	Provision of CSA publications	Public		
	Provision of data and as such: Website	Public		
	Provision of communication material in digital format	Public		

Appendix 3: Risk Evaluation Summary from DPO

RISK ASSESSMENT AND SECURITY MEASURE FOR PERSONAL DATA PROCESSING

Assessment of the level of risk for processing operation **Assessing the maturity of the EU cancer care infrastructure by sending questionnaires to care centre staff (CCI4EU project)** and a proposal for appropriate technical and organizational security measures.

Section I – Definition and Context of the Processing Operation

PROCESSING OPERATION DESCRIPTION	ANSWER	
Personal Data Processed	Contact information of the heads of the different centres (name, surname, institutional email address, work phone numbers)	
Processing Purpose	Sending survey to contact persons	
Data Subject	Care Centre Managers	
Processing Means	Data will be imported onto a password-protected online web tool used only by members of the CCI4EU consortium	
Recipients of Personal Data	Internal	CCI4EU consortium
	External	NONE
Data Processor Used	No data processor will be nominated. All personal data will be stored on in-house sever provide by TUD	

Section II – Evaluation of the Impact

Confidentiality impact assessment: Low
To a great extent, the personal data processed are already on public websites

Integrity impact assessment: Low
a loss of integrity could decrease the validity of the data collected for the CCI4EU project, but would in no way affect the data subjects

Availability impact assessment: Low
a loss of availability could decrease the validity of the data collected for the CCI4EU project, but would in no way affect the data subjects

IMPACT ASSESSMENT		
Confidentiality	**Integrity**	**Availability**
Low	Low	Low
	Overall Impact Evaluation	Low

Section III – Analysis of the Threats per Assessment Area

Network and Technical Resources threat probability: Low

- **Is any part of the processing of personal data performed through the internet? Yes**
  In the course of the project, data will be imported onto a password-protected online web tool used only by members of the CCI4EU consortium to assess the maturity of each participating CCI.
- **Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)? Yes**
  Only CCI4EU project members can access to data
- **Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service? No**
  Maturity model web site are not interconnected to other IT systems
- **Can unauthorized individuals easily access the data processing environment? No**
  Data are password protected
- **Is the personal data processing system designed, implemented or maintained without following relevant documented best practices? Yes**
  Information for data use are sent to data subject

Processes/Procedures related to the processing of personal data threat probability: Low

- **Are the roles and responsibilities with regard to personal data processing vague or not clearly defined? Yes**
  All CCI4EU members were designated as co-controllers.
- **Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined? Yes**
  A network utilisation policy was defined by each consortium member
- **Are the employees allowed to bring and use their own devices to connect to the personal data processing system? No**
  No personal devices can access or process data
- **Are the employees allowed to transfer, store or otherwise process personal data outside the premises of the organization? No**
  No data can be transfered oustide the consortium
- **Can personal data processing activities be performed without log files being created? No**
  A log of data access is retained

Parties/People involved in the processing of personal data threat probability: Low

- **Is the processing of personal data performed by an undefined number of employees? No**
  Only specific employees on the CCI4EU consortiun will access to personal data
- **Is any part of the data processing operation performed by a contractor/third party (data processor)? No**
  No data processing will be nominated
- **Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated? No**
  Employees of the consortium are well informed about personal data treatment

- **Is the personnel involved in the processing of personal data unfamiliar with security matters?** **No**
  Employees of the consortium are well informed about personal data treatment
- **Do the persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?** **No**
  Personal data are password protected

Business sector and scale of processing threat probability: **Low**

- **Do you consider your business sector as being prone to cyberattacks?** **No**
- **Has your organization suffered any cyberattack or other type of security breach over the last two years?** **No**
- **Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?** **No**
- **Does your processing operation concern a large volume of individuals and/or personal data?** **No**
- **Are there any security best practices specific to your business sector that have not been adequately followed?** **No**
  Seurity measures have benn followed

ASSESSMENT AREA	PROBABILITY	
Network and Technical Resources	Low	1
Processes/Procedures related to the processing of personal data	Low	1
Parties/People involved in the processing of personal data	Low	1
Business sector and scale of processing	Low	1
Overall Threat Occurrence Probability	Low (4)	

Section IV – Evaluation of Risk

	IMPACT LEVEL			
THREAT OCCURRENCE PROBABILITY		Low	Medium	High / Very High
	Low	X		
	Medium			
	High			

Section V – Organizational Security Measures

It should be noted that the adequacy of measures to specific risk levels should not be perceived as absolute. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk. Furthermore, the proposed list of measures does not take into account other additional sector specific security requirements, as well as specific regulatory obligations, arising for example from the ePrivacy Directive or the NIS Directive. In an attempt to further facilitate this procedure a mapping of the proposed group of measures with the ISO/IEC 27001:2013 security controls is also included.

Security policy and procedures for the protection of personal data

Measure Identifier	Measure Description	Risk level
A.1	The organization should document its policy with regards to personal data processing as part of its information security policy.	
A.2	The security policy should be reviewed and revised, if necessary, on an annual basis.	
	Related to ISO 27001:2013 - A.5 Security policy	

Roles and responsibilities

Measure Identifier	Measure Description	Risk level
B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	
B.2	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.	
	Related to ISO 27001:2013 - A.6.1.1 Information security roles and responsibilities	

Access control policy

Measure Identifier	Measure Description	Risk level
C.1	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.	
	Related to ISO 27001:2013 - A.9.1.1 Access control policy	

Resource/asset management

Measure Identifier	Measure Description	Risk level
D.1	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).	
D.2	IT resources should be reviewed and updated on regular basis.	
	Related to ISO 27001:2013 - A.8 Asset management	

Change management

Measure Identifier	Measure Description	Risk level
E.1	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.	
E.2	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.	
	Related to ISO 27001:2013 - A. 12.1 Operational procedures and responsibilities	

Data processors

Measure Identifier	Measure Description	Risk level
F.1	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy.	
F.2	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.	
F.3	Formal requirements and obligations should be formally agreed between the data controller and the data processor. The data processor should provide sufficient documented evidence of compliance.	
	Related to ISO 27001:2013 - A.15 Supplier relationships	

Incidents handling / Personal data breaches

Measure Identifier	Measure Description	Risk level
G.1	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.	
G.2	Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.	
	Related to ISO 27001:2013 - A.16 Information security incident management	

Business continuity

Measure Identifier	Measure Description	Risk level
H.1	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).	
	Related to ISO 27001:2013 - A. 17 Information security aspects of business continuity management	

Confidentiality of personnel

Measure Identifier	Measure Description	Risk level
I.1	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.	
	Related to ISO 27001:2013 - A.7 Human resource security	

Training

Measure Identifier	Measure Description	Risk level
J.1	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	
	Related to ISO 27001:2013 - A.7.2.2 Information security awareness, education and training	

Access control and authentication

Measure Identifier	Measure Description	Risk level
K.1	An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.	
K.2	The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.	
K.3	An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.	
K.4	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.	
	Related to ISO 27001:2013 - A.9 Access control	

Logging and monitoring

Measure Identifier	Measure Description	Risk level
L.1	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).	
L.2	Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source	
	Related to ISO 27001:2013 - A.12.4 Logging and monitoring	

Server/Database security

Measure Identifier	Measure Description	Risk level
M.1	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.	
M.2	Database and applications servers should only process the personal data that are actually needeeds to process in order to achieve its processing purposes.	

Measure Identifier	Measure Description	Risk level
	Related to ISO 27001:2013 - A. 12 Operations security	

Workstation security

Measure Identifier	Measure Description	Risk level
N.1	Users should not be able to deactivate or bypass security settings.	
N.2	Anti-virus applications and detection signatures should be configured on a weekly basis.	
N.3	Users should not have privileges to install or deactivate unauthorized software applications.	
N.4	The system should have session time-outs when the user has not been active for a certain time period.	
N.5	Critical security updates released by the operating system developer should be installed regularly.	
	Related to ISO 27001:2013 - A. 14.1 Security requirements of information systems	

Network/Communication security

Measure Identifier	Measure Description	Risk level
O.1	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).	
	Related to ISO 27001:2013 - A.13 Communications Security	

Back-ups

Measure Identifier	Measure Description	Risk level
P.1	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.	
P.2	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	
P.3	Execution of backups should be monitored to ensure completeness.	
P.4	Full backups should be carried out regularly.	
	Related to ISO 27001:2013 - A.12.3 Back-Up	

Mobile/Portable devices

Measure Identifier	Measure Description	Risk level
Q.1	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.	
Q.2	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	
Q.3	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.	
	Related to ISO 27001:2013 - A. 6.2 Mobile devices and teleworking	

Application lifecycle security

Measure Identifier	Measure Description	Risk level
R.1	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.	
R.2	Specific security requirements should be defined during the early stages of the development lifecycle.	
R.3	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.	
R.4	Secure coding standards and practises should be followed.	
R.5	During the development, testing and validation against the implementation of the initial security requirements should be performed.	
	Related to ISO 27001:2013 - A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes	

Data deletion/disposal

Measure Identifier	Measure Description	Risk level
S.1	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.	
S.2	Shredding of paper and portable media used to store personal data shall be carried out.	
	Related to ISO 27001:2013 - A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment	

Physical security

Measure Identifier	Measure Description	Risk level
T.1	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.	
	Related to ISO 27001:2013 - A.11 – Physical and environmental security	

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 the European Commission. Neither the European Union nor the granting authority can be held responsible for them.