FiERCE
MAKING SPACE FOR GREEN SOLUTIONS

D7.3 - Data Management Plan – 1st period, Interim version

Q-PLAN INTERNATIONAL

30/04/2026

Funded by the European Union

Document Information

Issued by:	Q-PLAN INTERNATIONAL
Issue date:	30/04/2026
Due date:	30/04/2026
Work package leader:	Q-PLAN INTERNATIONAL
Dissemination level:	Public

Document History

Version	Date	Modifications made by
1.1	30/01/2026	**First version issued by Q-PLAN and shared with partners for input**
1.2	27/02/2026	**Second version incorporating input, addressing partners feedback and shared for final revision**
2.0	30/04/2026	**Final version ready to be submitted**

Authors

First Name	Last Name	Beneficiary
Christina	Balla	Q-PLAN INTERNATIONAL
Paraskevi	Rampota	Q-PLAN INTERNATIONAL
Vasiliki	Avgikou	Q-PLAN INTERNATIONAL

In case you want any additional information, or you want to consult with the authors of this document, please send your inquiries to: balla@qplan-intl.gr

Quality Reviewers

First Name	Last Name	Beneficiary
Georgia	Simadi	DREVEN
Costanza	Crivelli Visconti	NOVASPACE
Luce	Kaiser	NOVASPACE

Executive Summary

This document constitutes the interim version of the Data Management Plan (DMP), building upon the initial version (deliverable D7.2) in the framework of FIERCE project. FIERCE is a 3-year Coordination and Support Action, funded by the European Union's (EU) Horizon Europe Framework Programme for Research and Innovation Horizon Europe under Grant Agreement No 101177496.

With a mission to accelerate Europe's green and digital transition, FIERCE will mobilize 2.5 million EUR in financial support for 70 SMEs, start-ups and scale-ups to fuel the development, demonstration and commercialization of green space-enabled solutions. On top of that, FIERCE will support 140 SMEs with specialised technical and business advisory to design business solutions and engage in process innovation using downstream space data in areas such as circularity, raw materials, environmental monitoring and corporate sustainability. In parallel, FIERCE will enable a series of local entrepreneurship initiatives driven by innovation intermediaries and business support networks aimed at creating even more opportunities for space-enabled green innovation through synergies with regional industrial, research and market actors.

In this context, the interim version of the project's DMP reviews and revises, when necessary, the overall methodological principles pertaining to the management of the data collected and/or generated in the framework of FIERCE, safeguarding sound and ethical data management for the entire duration of the project. Moreover, it provides an updated overview of FIERCE's data, as identified in this interim stage of the project, along with information on the methodology pertaining to their management as well as making them Findable, Accessible, Interoperable and Re-usable (FAIR).

This first updated version of the DMP is the second of three versions of the FIERCE's Data Management Plan to be produced in the course of the project and will serve as a living document (D7.2 Data Management Plan – Initial Version delivered in M3 is updated to D7.3 Data Management Plan – Interim Version in M18 and ultimately fixed as D9.1 Data Management Plan – Final Version in M36). Along these lines, the initial DMP has been updated and will be further elaborated during the project to reflect an accurate, up-to-date and ultimately comprehensive plan for managing the data that will be collected, and/or generated by the project across its entire life cycle, both during and after the completion of FIERCE.

Table of Contents

EXECUTIVE SUMMARY **3**

1. INTRODUCTION **7**

2. DATA SUMMARY **10**

2.1 PURPOSE OF DATA COLLECTION / GENERATION AND ITS RELATION TO THE OBJECTIVES OF THE PROJECT 10
2.2 TYPES AND FORMATS OF COLLECTED / GENERATED DATA 11
2.2.1 Data collected/ generated through direct input methods 12
2.2.2 Data generated through the use of the FIERCE digital toolbox 15
2.2.3 Data collected / generated from dissemination, communication and clustering activities 16
2.3 ORIGIN OF DATA AND RE-USE OF PRE-EXISTING DATA 18
2.4 EXPECTED SIZE OF DATA 18
2.5 DATA UTILITY 20

3. FAIR DATA **22**

3.1 MAKING DATA FINDABLE, INCLUDING PROVISIONS FOR METADATA 22
3.1.1 Data discoverability and identification mechanisms 22
3.1.2 Naming conventions 22
3.1.3 Metadata allowing discovery 23
3.1.4 Standards for metadata creation 24
3.1.5 Search keywords included in the metadata 25
3.1.6 Offering metadata that can be harvested and indexed 26
3.2 MAKING DATA ACCESSIBLE 26
3.2.1 Repository 26
3.2.2 Data 27
3.2.3 Metadata 33
3.3 MAKING DATA INTEROPERABLE 35
3.4 INCREASE DATA RE-USE 36
3.4.1 Documentation for validating data analysis and facilitating data re-use 36
3.4.2 License schemes to permit the widest use possible 37
3.4.3 Availability for re-use 38
3.4.4 Data provenance 40
3.4.5 Data quality assurance processes 40

4. ALLOCATION OF RESOURCES **42**

4.1 ESTIMATED COSTS FOR MAKING DATA FAIR 42
4.2 DATA MANAGEMENT RESPONSIBILITIES 44

5. DATA SECURITY **46**

6. ETHICAL ASPECTS AND OTHER PROCEDURES **48**

7. CONCLUSIONS AND WAY FORWARD **50**

8. ANNEXES 51
8.1 ANNEX I – INFORMED CONSENT FORM 51
8.2 ANNEX II – DATA SUBJECT REQUEST FORM 54
8.3 ANNEX III – RECORD OF PROCESSING ACTIVITIES 56

List of Figures

Figure 1: Typical DOI created by Zenodo 27
Figure 2: CC BY-SA 4.0 37
Figure 3: CC BY 4.0 37
Figure 4: CC BY-ND 4.0 37
Figure 5: CC BY-NC 4.0 38
Figure 6: CC BY-NC-ND 4.0 38

List of Tables

Table 1: Abbreviations 6
Table 2: FIERCE partners 7
Table 3:Expected size of data 19
Table 4: Data utility 20
Table 5: Good practices for data anonymisation 28
Table 6:Data availability 29
Table 7:Data accessibility 31
Table 8: Dublin core Metadata standard vocabulary 35
Table 9: Expected time that data will be made open through Zenodo 39
Table 10:Estimated costs for making data FAIR 42
Table 11:Data management responsibilities of FIERCES's partner per data collected/generated under each WP 45

List of Terms and Definitions

Table 1: Abbreviations

Abbreviation	Definition
CESSDA	Consortium of European Social Science Data Archives
DCMI	Dublin Core Metadata Initiative
DMP	Data Management Plan
DOI	Digital Object Identifier
DPO	Data Protection Officer
EEA	European Economic Area
FAIR	Findable, Accessible, Interoperable and Re-usable
GDPR	General Data Protection Regulation
HaDEA	European Health and Digital Executive Agency.
HTML	Hypertext Markup Language
OAI	Open Archives Initiative
OAI-PMH	Open Archives Initiative Protocol for Metadata Harvesting
PID	Persistent Identifier
PC	Project Coordinator
QA	Quality Assurance
QR	Quality Review
URL	Uniform Resource Locator
WP	Work Package
WPL	Work Package Leader
WTL	Work Task Leader

1. Introduction

The current document represents the interim version of the Data Management Plan of FIERCE, which is funded by the European Union's (EU) Horizon Europe Framework Programme for Research and Innovation Horizon Europe under Grant Agreement No 101177496.

With a mission to accelerate Europe's green and digital transition, FIERCE will mobilize 2.5 million EUR in financial support for 70 SMEs, start-ups and scale-ups to fuel the development, demonstration and commercialization of green space-enabled solutions. On top of that, FIERCE will support 140 SMEs with specialised technical and business advisory to design business solutions and engage in process innovation using downstream space data in areas such as circularity, raw materials, environmental monitoring and corporate sustainability. In parallel, FIERCE will enable a series of local entrepreneurship initiatives driven by innovation intermediaries and business support networks aimed at creating even more opportunities for space-enabled green innovation through synergies with regional industrial, research and market actors.

Overall, by fostering collaboration between SMEs and innovation intermediaries, the project will pave the way for a more informed policy landscape and accelerate the uptake of green, space-enabled innovations across Europe. Through these actions, FIERCE will act as a catalyst for driving sustainable growth, supporting the EU's green and digital transformation while addressing key challenges faced by SMEs in leveraging space-based solutions.

To this end, the consortium of FIERCE brings together a complementary and interdisciplinary group of 7 partners across 7 different countries within the EU and beyond, as presented in the table which follows.

Table 2: FIERCE partners

Partner Role*	Partner No	Partner Name	Partner short name	Country
COO	1	Q-PLAN INTERNATIONAL	Q-PLAN	Greece
BEN	2	NOVASPACE GMBH	NVS-DE	Germany
AE	2.1	NOVASPACE SRL	NVS-BE	Belgium
BEN	3	FUNDINGBOX ACCELERATOR SP ZOO	FBA	Poland
AE	3.1	FUNDINGBOX COMMUNITIES SL	FBC	Spain
BEN	4	EUROPA MEDIA SZOLGALTATO NONPROFITKOZHASZNU KFT	EMNP	Hungary
BEN	5	TECH TOUR GLOBAL EOOD	TTG	Bulgaria
BEN	6	EIT RAW MATERIALS GMBH	EIT-RM	Germany

BEN	7	DRAXIS RESEARCH VENTURES ASTIKI MI KERDOSKOPIKI ETAIRIA	DREVEN	Greece

* COO = Coordinator, BEN = Beneficiary, AE = Affiliated Entity

All partners of FIERCE consortium adhere to sound data management principles in order to ensure that the meaningful data collected, processed and / or generated throughout the duration of the project are well-managed, archived and preserved, in line with the guidelines of the Horizon Europe Data Management Plan Template[1].

Along these lines, this interim version of the DMP aims to achieve the following objectives:

- Describe the data management lifecycle for the data collected and/or generated in the framework of FIERCE, serving as the key element of good data management.
- Outline the methodology employed to safeguard the sound management of the data collected, and/or generated as well as to make them Findable, Accessible, Interoperable and Re-usable (FAIR).
- Provide information on the data collected and/or generated and the way in which they will be handled during and after the end of the project along with the standards applied to this end.
- Describe details on how the data will be made openly accessible and searchable to interested stakeholders as well as its curation and preservation.
- Present information on the resources to be allocated so as to make data FAIR, clearly identifying responsibilities pertaining to data management, while addressing data security and ethical aspects.

With the above in mind, this interim version of the DMP is structured in 7 distinct chapters, as follows:

- Chapter 1 provides introductory information about the DMP, the context in which it has been elaborated as well as about its objectives and structure.
- Chapter 2 presents a summary of the data collected/generated during the activities of FIERCE including the purpose of its collection/ generation as well as its types and formats. Additionally, it outlines its origin, expected volume and the stakeholders that may find it useful.
- Chapter 3 describes the methodology that is applied in the framework of FIERCE in order to safeguard the effective management of data across their entire lifecycle, making it FAIR.

[1] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx

- Chapter 4 estimates the resources required for making the project's data FAIR, while also identifying data management responsibilities.
- Chapter 5 outlines the data security strategy applied within the context of FIERCE along with the respective secure storage solutions employed.
- Chapter 6 addresses ethical aspects as well as other relevant considerations pertaining to the data collected/ generated during the implementation of the project.
- Chapter 7 concludes with the next steps foreseen in the framework of the project with respect to its data management plan.

Annexed in the document are (i) the templates for the Informed Consent Form (Annex I) and (ii) the Data Subject Request Form (Annex II) as well as (iii) the Record of Processing Activities (Annex III) which are used during the implementation of the project's activities to ensure compliance with relevant applicable EU and national regulation(s).

The methodology of FIERCE for data management builds on know-how, tools and templates that were developed internally by Q-PLAN as well as on good practices and templates from the literature (such as the Horizon Europe Data Management Plan Template). As in previous EU-funded projects, tailored modifications to the methodology were implemented for FIERCE as well, in order to comply with the GA conditions and the particularities of the project. Along these lines, this deliverable presents the adjusted methodology as it was further developed and applied in the context of FIERCE, as well as presents the results from its application during the project.

Also note that the DMP is not a fixed document. It evolves during the lifespan of the project and will be further elaborated and updated throughout the duration of FIERCE (i.e., as D9.1 Final Version in M36). Additional ad hoc updates may also be realised (if necessary), in order to include new data, better detail and/or reflect changes in the methodology or other aspects relevant to their management (such as costs for making data FAIR, size of data, etc.), changes in consortium policies and plans or other potential external factors. Q-PLAN is responsible for the elaboration of the DMP and with the support of all partners will update and enrich it, when required.

2. Data summary

FIERCE collects/ generates meaningful non-sensitive data that do not fall into any special categories[2] of personal data as those are described within the General Data Protection Regulation[3] (GDPR). This data may be quantitative, qualitative or a blend of those in nature and is analysed from a range of methodological perspectives with a view to producing insights that successfully feed FIERCE's activities, enabling us to deliver evidence-based results and ultimately achieve the objectives of the project.

With that in mind, the second chapter of the Data Management Plan (DMP) starts by explaining the purpose for which this data is collected/ generated and how it relates with FIERCE. It proceeds by describing the different types and formats of this data as well as its origin and expected volume, before concluding with an overview of potential stakeholders for whom it may prove useful for re-use.

2.1 Purpose of data collection / generation and its relation to the objectives of the project

In order to successfully meet its objectives and ensure the production of evidence-based results, FIERCE entails several activities during which data is collected/generated. The purpose for which this data is collected/ generated is interrelated with the objective of the activity during which it is produced.

In particular, these activities along with their objectives in the framework of FIERCE are as follows:

- Studying the current uses of downstream space data and services offered by EUSPA along with the success factors, barriers and support requirements of the SMEs.
- Investigation of SMEs' awareness regarding the potential of downstream space data and services for the development of green solutions as well as their capacity and skills to incorporate such data in their processes, products, services.
- Profiling of 8 local innovation ecosystems across the EU regarding their potential to conduce space-enabled green entrepreneurship, complemented by first-hand insights on existing or missing support opportunities.

[2] Special categories of personal data according to Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation) include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[3] Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

- Organisation of the Design Sprint to shape the results of our initial studies into the blueprints of our support programs and tools (scope, prerequisites, delivery methods, expected outcomes, etc.)
- Deployment and utilisation of the FIERCE digital toolbox in order to facilitate the delivery of the Advisory Services, the Transformation projects, etc., through the “open calls” portal, the Self-Assessment and Diagnosis tool, the Learning Hub, the Replication Toolkit and the FIERCE Network and Community functionality.
- Implementation of the Advisory Services, the Transformation Projects and the Ecosystem Building Programme to enable the SMEs’ green and digital transition using downstream space data.
- Implementation of the monitoring and evaluation activities to fuel the iterative improvement of the FIERCE support programmes (Advisory Services, Transformation Projects, Ecosystem Building Programme, etc.) and tools.
- Implementation of the FIERCE replication and scale-up activities to inspire others to drive the green and digital transition within their ecosystem through downstream space data.
- Design and deployment of activities to generate policy recommendations for more conducive SME support structures, policies and innovation ecosystems for space enabled green entrepreneurship at regional, national and EU level.
- Monitoring and assessment of the dissemination and communication activities of the project, with a view to maximising the project’s visibility and successfully conveying its value propositions and results to target audiences, as well as measuring the impact of the project’s relevant activities and accordingly fine-tuning FIERCE’s strategy in this respect.
- Creation and engagement of the Strategic Partners Network and the Advisory Board, with a view to systematically engaging diverse stakeholders in various project activities, receive their support on our programs and drive the wide-spread acceptance and replication of our results.

The following section provides further details on the different types and formats of data collected\generated during the project’s activities.

2.2 Types and formats of collected / generated data

FIERCE collects / generates data of various structures and formats. Along these lines, the data definition process used for this DMP is based on the source and the physical format of the data[4]. In particular, we define two main aspects: (i) the process under which the underlying data is created / captured which includes electronic texts documents, spreadsheets, questionnaires and transcripts, among others and (ii) the storage format of quantitative and qualitative data. Examples of this aspect

[4] Jakobsson, U., Braukmann, R., Lundgren M., Expert Tour Guide on Data Management. Retrieved from https://www.cessda.eu/Research-Infrastructure/Training/Expert-Tour-Guide-on-Data-Management/1.-Plan.

include easily accessible formats, such as postscripts (e.g., pdf, xps, etc.), machine readable formats (xml, html, etc.), spreadsheets, (e.g., xlsx, csv, etc.), text documents (e.g., docx, rtf, etc.), compressed formats (e.g., rar, zip, etc.) or any other format required by the objectives and methodology of the activity within the framework of which is produced.

Under this framework, special attention is paid in using open formats[5] (such as csv, pdf, zip, etc.) and/or machine-readable formats[6] (such as xml, json, rdf, html, etc.) when possible, to enhance the interoperability and re-use of data. In doing so, we are providing data that is easily readable and freely usable in any software program employed by third parties interested in utilizing the data.

The type and formats of the data collected / generated in the context of FIERCE can be divided into 3 categories:

- Data collected / generated by direct input methods (i.e. feedback from interviews and online surveys, feedback from the recipients of the support services and stakeholders, input from the Advisory Board Members, etc.).
- Data collected / generated through the FIERCE digital toolbox (e.g. data generated through the application forms, the Self-Assessment tool, etc).
- Data collected / generated from dissemination, communication and stakeholder engagement activities.

2.2.1 Data collected/ generated through direct input methods

Direct input methods, under the scope of FIERCE, involve methodologies for collecting data through desk research and interactions between consortium partners and external stakeholders, with the latter providing data to the former. Along these lines, external stakeholders undertake the role of a data subject that is a natural person whose personal data is being processed[7]. In particular, the identification and selection of suitable data subjects is based on purposeful sampling according to which, external stakeholders are identified and selected by consortium partners based on their role (e.g., SMEs, innovation intermediaries, etc.) and the objectives of the respective activity for which data is collected. In this context, quantitative and qualitative data is collected / generated during FIERCE:

[5] According to the Open Data Handbook: "*An open format is a file format with no restrictions, monetary or otherwise, placed upon its use and can be fully processed with at least one free/open-source software tool and it is not encumbered by any copyrights, patents, trademarks or other restrictions so that anyone may use it*".
[6] According to the Open Data Handbook: "*Machine readable formats are file formats that can be automatically read and processed by a computer. Machine-readable data must be structured data*".
[7] Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

- Quantitative data is numerical and acquired through counting or measuring[8]. Examples of quantitative data are the number of SMEs involved in interviews, the count of learning material, numerical responses from the EU wide survey, etc. This data may be represented by ordinal, interval or ratio scales and lend themselves to statistical manipulation.
- Qualitative data, sometimes referred to as categorical data, is data that can be arranged into categories based on physical traits or anything that does not have a number associated with it[9]. Moreover, interviews, surveys, application forms, feedback cards, etc. are all sources of qualitative data.

Additional details with respect to the different types and formats of data that is collected through direct input methods under the frame of FIERCE are provided below.

Identification of success factors, barriers and support requirements

At the early stages of the project, the partners focused on gaining a deep understanding of the current uses of downstream space data. Under this light, they went beyond typical desk research and engaged in 27 interviews with SMEs to reveal the success factors, the barriers they faced and the further support that they would need to keep improving their business in their respective fields. Data collected during interviews were mostly of qualitative nature and were recorded in the form of transcripts, encompassing all relevant information needed to conduct the analysis. On top of that, an EU-wide survey was deployed to non-space SMEs to assess their potential and capacity to integrate downstream space data into their processes. The survey responses were collected through Prolific, anonymised and saved in a spreadsheet format, before being made publicly available to all interested parties through Zenodo (please see the dataset here). The data was collected according to the "privacy policy for participants" of Prolific.

Profiling innovation ecosystems with potential to drive the space-enabled green transition

This section refers to the data that was collected through 28 interviews with innovation intermediaries in order to provide us with firsthand insights on their own ecosystem, regarding the existing and missing opportunities, the community engagement, policy initiatives and so on, with a view to enhancing our mapping and profiling exercise for 8 local innovation ecosystems across EU. Data collected during interviews were mostly of qualitative nature and were captured in the form of video recordings and transcripts, encompassing all relevant information needed to conduct the analysis. The video recordings were conducted following a dedicated consent process to facilitate the transcription, and the video recordings were deleted after the results of the analysis.

[8] Neuman, W. L. (2014). Social research methods: Qualitative and quantitative approaches. Boston: Pearson.
[9] Neuman, W. L. (2014). Social research methods: Qualitative and quantitative approaches. Boston: Pearson.

Feedback and relevant ideas collected through the Design Sprint

The Design Sprint, organised in April 2025, engaged a set of selected stakeholders to co-define key aspects of the FIERCE support programmes and evaluation framework. Data was collected by means of written notes, minutes and pictures. The respective discussions, ideas, and relevant feedback were fully utilised for the elaboration of blueprints and project reports in the form of text documents (e.g. .docx). Visual evidence of the event taken for dissemination purposes were stored in picture or video format (e.g., .jpg, .mp4) and published in project deliverables or digital channels (e.g., via the social media accounts, website, etc.). All visual materials were collected and shared only after obtaining informed consent from participants (in-paper for the physical attendees and online for the online participants), ensuring compliance with data privacy regulations.

Deployment and finetuning of the FIERCE support programme\s

The deployment and fine-tuning of the FIERCE support programmes require the collection of data from the beneficiaries (i.e. advisory services beneficiaries, transformation projects beneficiaries, innovation intermediaries for the local entrepreneurship initiatives), the external service providers and the expert evaluators. Their data, input and feedback are used to implement and finetune our support programmes. Data to measure the impact and effectiveness of FIERCE programmes in driving green and digital transformation is also collected and assessed. In relation to the Advisory Services and the Transformation Projects, the beneficiaries' data are processed for the evaluation of their application forms, for the delivery of the Advisory Service/ implementation of their Transformation Project and for the provision of their feedback for improvement.

Data is collected during the Open Calls application process only for the purpose of selection and evaluation. The personal data (e.g. name, phone, etc.) is collected through the One Pass Platform (https://getonepass.eu/). Data collected through OnePass is managed according to the OnePass Terms of Service (https://getonepass.eu/trust/terms) and OnePass Privacy Notice for open call applicants (Privacy notice (open call)).

The evaluation of the application forms is done following the provisions of the Grant Agreement, with special emphasis on GDPR and ethics. The personal data that the beneficiaries provide us with for the delivery of the Advisory Services are handled according to the provision of the Privacy Notice that the beneficiaries were asked to read and submit (operated through Google Forms). The information they share for the delivery of the service is handled as confidential (when marked as such) in the form of text documents (e.g., .docx, pdf, etc.).

The same procedures will be applied also for the implementation of the Transformation Projects. The possibility to sign Non-Disclosure Agreements (within the framework of the Transformation Projects) before the commencement of the activities will be discussed on a case-by-case basis.

External service providers registering in the FIERCE Pool for the purpose of being matched with beneficiaries of the Transformation Projects are duly informed of the processing of their personal data through a dedicated Privacy Notice. This Privacy Notice is elaborated and made available by FBA and can be accessed here.

In addition, personal data will be collected from external experts engaged to carry out the evaluation of application forms submitted under the Financial Support Program. Such data processing is governed by the contractual arrangements concluded between the external experts and FBA. These

experts are likewise informed of the processing of their personal data through the relevant privacy notices issued by FBA, in accordance with applicable data protection legislation.

More information about the data management procedures that will be followed for the implementation of the Transformation Projects will become available at the final update of this deliverable in M36.

Implementation of replication and scale-up activities along with the creation of policy recommendations.

This dataset pertains to the data that will be collected through 30 additional interviews, (i) with SMEs (20) that have successfully completed their transformation projects, and (ii) with innovation intermediaries (10) that have deployed the most impactful local entrepreneurship initiatives. These interviews will enable the creation of case studies, factsheets, and ultimately 2 replication handbooks to facilitate the replication and scale up of our activities. Data collected during interviews are expected to be mostly of qualitative nature and will be recorded in the form of transcripts, encompassing all relevant information needed to conduct the analysis.

A dedicated EU policy roundtable will be organized by NVS and Q-PLAN with the support of partners and meaningful information and insights will be collected from discussions during its implementation. Provided data will contribute to the elaboration of the final set of “Policy Recommendations” and briefs as well as the refinement of FIERCE Replication Guide. Collected data will be mostly qualitative and will be written in text documents (e.g., .docx) and participant lists.

AB feedback

In the framework of setting up the FIERCE Advisory Board, personal data of AB experts (name and contact details) was collected by partners. During the implementation of the project, there are several key stages where guidance and feedback from experts on the field is needed to successfully multiply the respective activities. Data collected via AB activities and involvement, such as discussions and online performance review workshops, are expected to be comments and proposals written in standard document texts and spreadsheets.

Data collected/generated through direct input methods are stored in standard .docx as well as .xlsx formats. These formats allow the documentation of information from various files and documents in a single location. By doing so, it is possible to circulate raw data from transcripts, as well as text, images and other objects from other files to one document file or multiple tabs of a single spreadsheet. Moreover, both formats can be immediately converted into open and machine-readable formats (e.g. .xml and .csv) boosting the interoperability and re-usability of the data produced in the framework of FIERCE.

2.2.2 Data generated through the use of the FIERCE digital toolbox

A set of 7 tools is developed to support the deployment of the FIERCE support programmes as well as the community engagement and replication activities:

1. The Open Calls portal, materialized through the OnePass platform, allowing the interested SMEs to submit their applications for the Advisory Services program and the Transformation Projects program. As stated before, data collected through OnePass are managed according to the OnePass Privacy Notice (Privacy notice (open call)). The processing of data takes place on a legitimate basis pursuant to Art. 6 Regulation (EU) 2016/679 General Data Protection

Regulation - GDPR. OnePass allows users to maintain control of their own data. OnePass is striving towards data sovereignty and portability. Organizations that use OnePass are in control of their own data and can choose who they grant access to it. OnePass is built on privacy-by-design and with Self-Sovereign Identity (SSI) principles at its core such as transparency, user consent, data portability, identity control, and user protection.

2. The Open Call portals on the FIERCE website, serving as the main gateway to OnePass and encompassing the Open Calls' documentation. These portals are webpages and the data they generate refer to user activity which is captured by Google Analytics.
3. The Learning Hub, encompassing more than 50 learning sources and 10 web-based tools to build the capacity of SMEs, start-ups and scale ups to engage in space-enabled green entrepreneurship, curated from reputable sources. User data is tracked through Google Analytics integrated into the tool (and the whole website), to monitor the traction of Learning Hub and evaluate which courses gain more attention and which ones need to be replaced.
4. The Self-Assessment tool, enabling the definition of the SMEs' status and support needs (e.g. advisory services, training, financial support, etc.). The tool automates the initial needs analysis of the SMEs, which is further elaborated by the Mentors afterwards. The Tally platform is used to materialise the Self-Assessment tool and the personal data is handled according to Tally's privacy policy. Users are asked to read and accept both the FIERCE privacy policy and Tally's privacy policy before commencing the use of the tool. The data collected through the tool become available to the Lead Mentors (provided by EMNP in .xls form) in order to evaluate the needs of the beneficiaries. The Diagnosis Tool is operated through the Tally platform as well, following the same procedures as the Self-Assessment Tool.
5. The Replication and Policy Toolkit, serving as a reference point for the outcomes of our replication and policy activities such as the inspirational material (SME case studies, innovation ecosystem profiles) replication handbooks as well as policy insights and recommendations. The data that will be generated in this respect will refer to user activity and the documents' downloads by the website visitors. This data will be collected through Google Analytics, according to the respective Terms of Service https://www.google.com/analytics/terms/.
6. The FIERCE Network and Community Tool, serving as an open environment for search and interaction for the FIERCE community of SMEs, innovation intermediaries, investors, strategic partners. The tool is embodied through a dedicated LinkedIn group, called "The FIERCE Group - Making downstream space a mainstream place for innovators". Some analytics are reviewed for the group by LinkedIn, mostly with regards to member activity and member demographics (e.g. job title, industry, location, etc.).

2.2.3 Data collected / generated from dissemination, communication and clustering activities

Website analytics

FIERCE's website was launched in the beginning of 2025 and it collects data regarding visitors' statistics. When using FIERCE's website or subscribing to our newsletter, users are asked to give consent to the collection, storage, processing and use of their information. This data is mostly used for reporting purposes.

Visitor statistics data refers to anonymised data that is collected through Google Analytics. This includes data that is automatically collected via cookies from every person visiting the website. More specifically, it consists of information about the visitor's device used for accessing the website (e.g., web browser, IP address, time zone), and information on how visitors interact with the website. Detailed information on how our website collects and handles data is provided in FIERCE's Privacy Policy document, available here. The Privacy Policy including the Cookies Policy are both available on the project's website. This document provides details on how and when FIERCE will, in accordance with the GDPR, use and share the website visitors' or the newsletter recipients' information.

More details on the collection of data from newsletter subscribers are provided in a separate section below.

Social Media statistics (including Facebook, X, LinkedIn, and YouTube)

This data is collected/ generated through a periodic monitoring of the project's social media statistics (including Facebook, X, LinkedIn and YouTube) with a view to measuring and assessing the performance and results of the project's social media activity in terms of dissemination and communication. With that in mind, the data is both qualitative as well as quantitative in nature addressing the metrics reached on each channel (e.g., followers, impressions on X, likes, subscription to YouTube etc.). Data is stored in a Microsoft excel file(.xlsx) while at the same time the analysis of the results will be stored in a standard word document (.docx) in the framework of the respective deliverables.

Data collected from project events

This data will be collected during the implementation of the project through: (i) the different events (e.g., design sprint, roadshows, EU policy roundtable, etc.) organised by FIERCE (e.g. participant list) and (ii) the participation of FIERCE partners in relevant third-party events in order to reach out and engage stakeholders.

The data is collected to keep track of the results of the stakeholder engagement activities and provide the opportunity for project partners to report on these activities. Moreover, this data will be updated every time a partner attends an event, or a partner organises an event. Finally, the data is both quantitative and qualitative and is stored in a standard spreadsheet (.xlsx).

Newsletter subscription

A subscription form hosted on the project's website manages the collection of this data (list of emails) in which any interested stakeholder can freely provide his/ her email in a dedicated sign-up form so as to receive the most up-to-date news and outcomes of the project. A newsletter is sent to subscribers twice a year. This list is stored on MailChimp's server (http://mailchimp.com), which is used for e-mail campaigns and newsletters distribution. The email list will be used and protected according to MailChimp's Privacy Policy.

In parallel to Mailchimp recipients, a newsletter is sent to LinkedIn followers that have accepted to receive the FIERCE newsletter. The newsletter is being sent automatically through LinkedIn and no personal data is being collected by the dissemination manager (Q-PLAN).

Data from dissemination and communication activities

This data is collected through the periodic monitoring of the project's miscellaneous dissemination and communication activities such as attending events, etc. The purpose of collecting this data is to assess the outreach and efficiency of the dissemination activities during the implementation of the project. This data is both qualitative and quantitative in nature, recording all the activities that partners conduct and the events they organise and/or attend, as well as the statistics about the number of participants/ recipients and, when relevant, their characteristics (e.g., stakeholder type). Data is integrated and stored in a single excel file (.xlsx) in Q-PLAN's repositories.

2.3 Origin of data and re-use of pre-existing data

In the context of FIERCE, data is collected/ generated by partners as well as external stakeholders participating in the activities of the project and/ or using the FIERCE digital toolbox. With that in mind and aside consortium partners, external groups of stakeholders from which new data will originate include:

- SMEs, start-ups and scale-ups
- Innovation intermediaries
- Investors
- Policy makers at regional, national and EU level
- Researchers and academia
- EU-wide networks
- Others

Moreover, pre-existing data will be utilised within the context of FIERCE as well. In particular, outputs from EU-funded projects such as InnORBIT, national projects and other relevant initiatives in a large extent will provide a solid basis for FIERCE. The FIERCE consortium will strive to make the most of and advance the work and results of these projects. Such activities include desk research on existing project reports for our WP1 activities as well as sources to feed the FIERCE Learning Hub. Finally, consortium partners' internal knowledge, experience and expertise from their participation in other projects and initiatives will directly and indirectly support the implementation of activities throughout the project.

2.4 Expected size of data

FIERCE entails a series of activities to facilitate the design, deployment, evaluation, validation and fine-tuning of the FIERCE support programs. With that in mind, the table that follows presents the different activities implemented during the course of the project in which data is collected/generated, the types and formats of the data as well as the expected size of the data.

Table 3:Expected size of data

No	Name of activity	Data	Type of data	Format of data	Size of data
1	State-of-play of downstream space applications	Data from interviews with 27 stakeholders	Interview transcripts and signed consent forms	.docx,	~2 MB
2	Studying the potential of non-space SMEs to integrate downstream space	Data from survey implemented with stakeholders (545 responses collected)	Survey responses collected from Prolific	.xlsx .csv	~15MB
3	Profiling the innovation ecosystems	Data from interviews with 16 stakeholders	Interview transcripts and signed consent forms	.docx .xlsx .pdf	~10 MB
4	Design Sprint	Ideas, concepts and visuals collected during the Design Sprint	Notes, documents, info about participants; images from the event	.docx .xlsx .pdf .jpg	~2GB
5	Development of FIERCE toolbox	Direct data input (open call applications, self-assessment tool)	Application form input, textual documents	Web data in various formats	10 GB
6		Data generated from the users	Log files, query data, etc.	Web data in various formats	20 GB
7	Delivery and fine-tuning of the FIERCE support programs (Advisory Services, Transformation Projects, Ecosystem Building program)	Data for the delivery and improvement of the programs	Data from the evaluation and selection of applications, Transformation roadmaps, data needed to deliver the service, feedback forms	.docx .xlsx .pdf	1-5 GB
9	Replication and Policy	Data collected during the replication and policy activities	Data from interviews, insights from policy roundtable,	.docx .xlsx .jpg/.png	10-20 GB

No	Name of activity	Data	Type of data	Format of data	Size of data
			photos from the event, list of stakeholders to send the handbooks and policy briefs		
11	Monitoring and assessment of the dissemination and communication activities and results	Social media statistics	Quantitative data	.xlsx	~10MB
12		Website analytics	Spreadsheets	.xlsx	~100KB
13		Newsletter subscriptions	Spreadsheets	.xlsx	~100KB
14		Data collected from events	Spreadsheets	.xlsx	~1MB
15		Data from dissemination and communication activities	Spreadsheets	.xlsx	~1MB

2.5 Data utility

The stakeholders that may find meaningful utility for the data to be collected/ generated by the project along with the benefits that could arise for them by utilizing this data, are concisely presented in the table that follows.

Table 4: Data utility

Stakeholder Groups	Data utility
SMEs (start-ups, scale-ups, entrepreneurs)	SMEs could mostly find value in the analysis of our datasets, such as the success factors or barriers for integrating downstream space or the analysis of the innovation ecosystem around them.
Innovation intermediaries	Innovation intermediaries would benefit mostly from the analysis of our datasets to deeply understand the status and pain points of the SMEs focused on space enabled green entrepreneurship, as well as the available opportunities of the broader support system.
Research and Academia	Researchers could use the analyzed results of our datasets to understand the scientific and technological niches that are of high interest not only to SMEs

Stakeholder Groups	Data utility
	but also to policy. This could enable them to better shape the focus of their research into the market needs.
Policy-makers	Throughout its duration, FIERCE is set on collecting and producing quantifiable evidence on the effectiveness and impact of the project's support programs, with a view to fostering the space enabled green and digital entrepreneurship. Data generated to this end, may be of great utility for stakeholders who design, implement and/ or fund relevant policies.
Project partners	The data collected/ generated during FIERCE is the corner stone for project partners to produce evidence-based results and ultimately achieve the objectives of the project. Indeed, this data will enable the co-design, deployment, validation and roll-out of the FIERCE support programs. At the same time, this data may be meaningful for project partners beyond the end of the project as well, enabling them to build and capitalise upon interesting ideas and opportunities that may emerge to ensure the long-term sustainability of the FIERCE support programs.

3. FAIR DATA

The Guidelines on Data Management[10] of the Commission emphasise the importance of making the data produced by projects funded under Horizon Europe Findable, Accessible, Interoperable as well as Reusable (FAIR), with a view to ensuring its sound management. This means using standards and metadata to make data discoverable, specifying data sharing procedures and which data will be open, allowing data exchange via open repositories as well as facilitating the reusability of the data.

With that in mind, the following sections of the DMP lay out the methodology followed in the framework of FIERCE with respect to making data findable, accessible and interoperable as well as ensuring their preservation and open access, with a view to increasing its re-use.

3.1 Making data findable, including provisions for metadata

3.1.1 Data discoverability and identification mechanisms

FIERCE places special emphasis in enhancing the discoverability of the data collected/ generated during the course of its activities. Open data produced during the implementation of the project will be locatable by means of a standard identification mechanism. Indeed, FIERCE will be able to assign globally resolvable Persistent Identifiers (PIDs) on any open data (more information on open data as well as the respective repositories we plan on employing in the context of the project are provided on section 3.2). An identifier is a unique identification code that is applied to a dataset, so that it can be unambiguously referenced. For example, a catalogue number is an identifier for a particular specimen and an ISBN code is an identifier for a particular book. PIDs are simply maintainable identifiers that allow for permanent reference to a digital object. In other words, PIDs are a way of giving digital resources, such as documents, images and data records, a unique and persistent reference number.

At the same time, data that is not open will be deposited in a searchable resource (i.e., google drive) and well-tailored identification mechanisms will be utilised as well, in the form of standard naming conventions that will safeguard their consistency and make them easily locatable for partners within the frame of the project. Along these lines, the following subsection provides further analysis on naming conventions and versioning.

3.1.2 Naming conventions

Following a consistent set of naming conventions in the development of the project's data files can greatly enhance their searchability. With that in mind, FIERCE creates consistent data file names that

[10] European Commission, H2020 Programme, Guidelines on FAIR Data Management in Horizon 2020, (2016), https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

provide clues to their content, status and versioning, while also increasing their discoverability. In doing so, project partners as well as interested stakeholders can easily identify a file as well as classify and sort them.

According to the UK Data Archive (UK Data Service, 2017b), a best practice in naming convention is to create brief yet meaningful names for data files, that facilitate classification. The naming convention should avoid the utilisation of spaces, dots and special characters (such as & or!), whereas the use of underscores is endorsed, to separate elements in the data file name and make them understandable. At the same time, versioning should be a part of a naming convention to clearly identify the changes and edits in a file.

With that in mind and to facilitate the reference of the datasets that will be produced during its implementation, FIERCE employs a standard naming convention that integrates versioning and takes into account the possibility of creating multiple datasets during an activity that entails data collection/generation. Indeed, FIERCE's naming convention considers this issue and addresses it by employing a unique element that captures the number of datasets that are produced under the same activity.

In particular, the naming convention employed by the project is described below.

[Name of project] _ [Name of Study] _ [Number of dataset] _ [Issue Date] _ [Version number]

Name of project: FIERCE

Name of Study: A short version of the name of the activity for which the dataset is created.

Number of dataset: An indication of the number assigned to the dataset.

Issue Date: The date on which the latest version of the dataset was modified (YYYY.MM.DD.).

Version number: The versioning number of a dataset.

With the above in mind, some indicative examples to showcase the naming structure applied in the context of FIERCE are provided below:

FIERCE _Successfactorsinterviews_Dataset1_2025.02.28_v1 – The first dataset generated from the interview transcripts of task 1.1. This is the first version of the dataset that was last modified on the 28th of February 2025.

Versioning of information makes a revision of datasets uniquely identifiable and can be used to determine whether and how data changed over time and to define specifically which version the creators/editors are working with. Moreover, effective data versioning enables understanding if a newer version of a dataset is available and which are the changes between the different versions allowing for comparisons and preventing confusion. In this context, a clear version number indicator is used in the naming convention of every data file produced during FIERCE in order to facilitate the identification of different versions.

3.1.3 Metadata allowing discovery

In addition to consistent naming conventions and versioning, the project also follows a metadata-driven approach so as to allow discovery and further increase the searchability of the data, while also

facilitating its understanding and re-use. Metadata is defined as “data about data” or “information about information”[11]. It is usually structured textual information that describes the creation, content, or context of a digital resource – be it a single file, part of a single file, or a collection of many files. Metadata is the glue which links information and data across the world wide web. It is the tool that helps people to discover, manage, describe, preserve, and build relationships with and between digital resources [12].

In particular, three distinct types of metadata exist[13], as presented below:

- Descriptive metadata, used to identify and describe collections and related information resources. Descriptive metadata at the local level helps with searching and retrieving. In an online environment, descriptive metadata helps to discover resources. Most of the times includes information such as the title, author, date, description, identifier, etc.
- Administrative metadata is used to facilitate the management of information resources. It is helpful for both short-term and long-term management and processing of data. This is information that will not usually be relevant to the public but will be essential for staff to manage collections internally. Such metadata may be location information, acquisition information, etc.
- Structural metadata enables navigation and presentation of electronic resources. It documents how the components of an item are organised. Examples of structural metadata could be the way in which pages are ordered to form chapters of a book, a photograph that is included in a manuscript or a scrapbook or the JPEG and TIF files that were created from the original photograph negative, linked together.

With that in mind, data produced/ used during FIERCE is discoverable with metadata suitable to its content and format. The project employs metadata standards to produce rich and consistent metadata with a view to supporting the long-term discovery, use and integrity of its data. More details on the metadata standards adopted by FIERCE are provided on the following subsection.

3.1.4 Standards for metadata creation

FIERCE employs standards for creating metadata for data collected/ generated by the project, with a view to describing it with rich metadata and thus improving their discoverability and searchability. In result, effective searching, improved digital curation and easy sharing will be realised. In addition, the metadata standards applied enable the integration of metadata from a variety of sources into other technical systems.

With that in mind, for FIERCE’s openly available data the metadata standards provided by Zenodo will be used. Zenodo (https://zenodo.org/) is an open repository developed under the European

[11] Huxley, L., & Jacobs, N. (2004). Online information services in the Social Sciences. Oxford: Chandos.
[12] Foulonneau, M., & Riley, J. (2008). Metadata for digital resources: Implementation, systems design and interoperability. Oxford: Chandos.
[13] Caplan, P. (2003). Metadata fundamentals for all librarians. Chicago: American Library Association.

OpenAIRE programme and operated by CERN. The repository along with its metadata standards have been adopted and are being used by numerus research communities, enabling them to deposit research papers, datasets, software, reports as well as other research outputs. Along these lines, Zenodo creates metadata to accompany the datasets that are uploaded to the repository, extending their reach to a wider audience of interested stakeholders. This metadata can be exported in several standard formats, including open and machine-readable ones (such as MARCXML, Dublin Core, and DataCite Metadata Schema), following the guidelines of OpenAIRE and are stored by Zenodo in JSON-format according to a defined JSON schema[14].

Project data not open, will also be annotated with open and machine-readable metadata following the Dublin Core Metadata standard. The Dublin Core Metadata element set (certified with the ISO Standard 15836) is a standard which can be easily understood and implemented and as such, is one of the best-known metadata standards. It was originally developed as a core set of elements for describing the content of web pages and enabling their search and retrieval. Among the reasons for selecting this standard is also the fact that Zenodo is compatible with Dublin Core metadata formats and thus any initially closed data, that may become open at a later stage (e.g., due to a change in the consortium's policy), will not lose its metadata. With that said, the Dublin Core metadata standard is a simple yet effective set for creating rich metadata that will describe a wide range of resources. The fifteen element "Dublin Core" described in this standard is part of a larger set of metadata vocabularies and technical specifications maintained by the Dublin Core Metadata Initiative (DCMI)[15]. The full set of vocabularies also includes sets of resource classes, vocabulary encoding schemes, and syntax encoding schemes. An online metadata generator will be used to produce the different metadata elements required (dublincoregenerator.com).

3.1.5 Search keywords included in the metadata

The project's data will be provided with search keywords with a view to optimizing its re-use by interested stakeholders during its entire lifetime. With that in mind, the metadata standards employed by FIERCE provide opportunities for tagging the data collected/generated and its content with keywords. In general, keywords are a subset of metadata and include words and phrases used to name data. In the context of FIERCE, keywords are used to add valuable information to the data collected/generated as well as to facilitate the description and interpretation of its content and value.

Along these lines, the project's strategy on keywords is underpinned by the following principles:

- The who, the what, the when, the where, and the why should be covered
- Consistency among the different keyword tags needs to be ensured
- Relevant, understandable and clear keywording ought to be sought

[14] For more information on the JSON format and the JSON schema visit the following website: http://json-schema.org/

[15] Retrieved from: https://www.dublincore.org/

In general, the keywords will comprise terms related to space-enabled green entrepreneurship. The keywords will accurately reflect the content of the datasets and avoid words used only once or twice within them.

3.1.6 Offering metadata that can be harvested and indexed

We know that the wild diversity of the metadata accompanying open data across the plethora of online repositories (e.g. disciplinary archives, institutional repositories, open access journals) can serve as barriers for their findability and sharing amongst different research communities. This is why in the context of FIERCE we have aligned our metadata creating approach with the Open Archives Initiative (OAI), which promotes the use of a standard protocol for metadata harvesting, designed for better sharing and retrieval of data residing in distributed repositories. This protocol, namely the Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH)[16] promotes interoperability standards that facilitate efficient dissemination of data amongst diverse communities[17].

All structured metadata linked to the project's open data will be offered in a way that can be exported and harvested via the OAI-PMH thanks to the standards we adopt for metadata creation (see section 3.1.4). The same standards will also help us produce metadata that facilitate indexing. For instance, the use of the Dublin Core Metadata Standard (as further elaborated in section 3.3) provides a vocabulary of concepts with definitions in open-machine readable formats that enable easier indexing of metadata. Along these lines, there are several tools[18] which implement the Archives Initiative Protocol for Metadata Harvesting, such as Arc source, EnhancedOAIServer and eprints.org, and can be used for harvesting our data by different repositories.

FIERCE's openly available data will be uploaded in Zenodo, which is in line with FAIR principles, including "To be Findable" principle. Metadata of each record uploaded in Zenodo is indexed and searchable directly in Zenodo's search engine immediately after publishing. Metadata of each record is sent to DataCite servers during DOI registration and indexed there.

3.2 Making data accessible

3.2.1 Repository

The data produced by FIERCE and deemed open for sharing and re-use, will be deposited to and securely stored by Zenodo (www.zenodo.org), which constitutes an open data repository and has been specifically selected to enable access to the project's open data free of charge. In fact, Zenodo builds and operates a simple service that enables researchers, scientists, EU projects and institutions, among others, to share and showcase research results (including data and publications) that are not

[16] Retrieved from: https://www.openarchives.org/pmh/

[17] Corrado, E.M. (2005) 'The importance of open access, open source, and open standards for libraries', Issues in Science and Technology Librarianship.

[18] For more information about the tools implementing the OAI-PMH: https://www.openarchives.org/pmh/tools/

part of the existing institutional or subject-based repositories of the research communities. It accepts any file format, promotes peer-reviewed openly accessible research, allows the creation of own collections and it is available free of charge both for FIERCE to upload and share data as well as for other stakeholders to explore, download and re-use this data.

Moreover, as a digital repository, Zenodo registers Digital Object Identifiers (DOIs) for all submitted data through DataCite[19], which is the leading global non-profit organisation that provides PIDs (and specifically DOIs) for research data and preserves these submissions using the safe and trusted foundation of CERN's data centre, alongside the biggest scientific dataset in the world, the LHC's 100PB Big Data store[20].This means that the data preserved in Zenodo will be accessible for years to come, and the DOIs will function as perpetual links to the resources. DOIs remain valuable since they are future proofed against Uniform Resource Locator (URL) or even protocol changes, through resolvers (such as DOI[21]). With that in mind, an example of a DOI retrieved from this open repository follows the structure illustrated by Figure 1.

Figure 1: Typical DOI created by Zenodo

3.2.2 Data

Openly available and closed data

FIERCE in line with FAIR principles of data management in the context of Horizon Europe, adopts the good practice of making data as open as possible and as closed as necessary. This calls for partners to disseminate their data that have the potential to offer long-term value to external stakeholders and do not harm the confidentiality and privacy of the stakeholders that contributed to the collection/ generation of this data, maximising the beneficial impact of FIERCE.

Only anonymised and aggregated data will be made open to ensure that data subjects cannot be identified in any reports, publications and/or datasets resulting from the project. The relevant project partner in each case will undertake all the necessary anonymisation procedures to anonymise the data in such a way that the data subject is no longer identifiable (more details on data management responsibilities are provided in Section 5.2).

To this end, it is important to keep in mind that during the process of data anonymisation, data identifiers need to be removed, generalised, aggregated or distorted. Moreover, anonymisation is different than pseudonymisation, which falls under a distinct category in the GDPR - anonymisation theoretically destroys any way of identifying the data subject, while pseudonymisation allows for the data subject to be re-identified with additional information. Along these lines, the table which follows provides a list of good practices for the anonymisation of quantitative and qualitative data derived

[19] For more information on DataCite: https://www.datacite.org/
[20] Retrieved from: https://www.software.ac.uk/tags/zenodo
[21] Retrieved from: http://dx.doi.org/

from the tour guide on data management of the Consortium of European Social Science Data Archives (CESSDA).

Table 5: Good practices for data anonymisation

Type of data	Good practices
Quantitative data	• Remove or aggregate variables or reduce the precision or detailed textual meaning of a variable. • Aggregate or reduce the precision of a variable such as age or place of residence. As a general rule, report the lowest level of geo-referencing that will not potentially breach respondent confidentiality. • Generalise the meaning of a detailed text variable by replacing potentially disclosive free-text responses with more general text. • Restrict the upper or lower ranges of a continuous variable to hide outliers if the values for certain individuals are unusual or atypical within the wider group researched.
Qualitative data	• Use pseudonyms or generic descriptors to edit identifying information, rather than blanking-out that information. • Plan anonymisation at the time of transcription or initial write-up, (longitudinal studies may be an exception if relationships between waves of interviews need special attention for harmonised editing). • Use pseudonyms or replacements that are consistent within the research team and throughout the project. For example, using the same pseudonyms in publications and follow-up research. • Use 'search and replace' techniques carefully so that unintended changes are not made, and misspelt words are not missed. • Identify replacements in text clearly, for example with [brackets] or using XML tags such as <seg>word to be anonymised</seg>. • Create an anonymisation log (also known as a de-anonymisation key) of all replacements, aggregations or removals made and store such a log securely and separately from the anonymised data files.

Source: Tour guide on data management of the CESSDA[22]

[22] Retrieved from: https://www.cessda.eu/Research-Infrastructure/Training/Expert-Tour-Guide-on-Data-Management/5.-Protect/Anonymisation

With that in mind, the following table presents the data collected/generated during the course of the project that will be made openly available. In case certain data cannot be shared (or need to be shared under restrictions), a justification for that choice is provided.

Table 6:Data availability

No	Data	Availability	Notes
1	State-of-play of downstream space applications	Open & Closed	Aggregated data and the results of the analysis will be open; data sources (e.g. interviews and information from confidential/ non-open documents) will be restricted to Partners
2	Studying the potential of non-space SMEs to integrate downstream space	Open	Raw data (answers collected directly from Prolific) are available on Zenodo here On top of that, aggregated, anonymised data will be made openly available.
3	Profiling the innovation ecosystems	Open & Closed	Aggregated data and the results of the analysis will be open; data sources (e.g. interviews and information from confidential/ non-open documents) will be restricted to Partners
4	Design Sprint	Open	This refers to processed data by nature (the analysis from the notes and minutes taken during the session after anonymisation of opinions/ input).
5	Development and utilisation of FIERCE toolbox	Closed	Since they can contain confidential business information (e.g. from open call applications, input in the self-assessment tool, etc.)
6	Delivery and fine-tuning of the FIERCE support programs (Advisory Services, Transformation Projects, Ecosystem Building program)	Closed	Raw data closed, since they can contain confidential business information. Aggregated anonymised statistical data will be provided as "sensitive" in the framework of the associated deliverables (meaning available only to the consortium and the EC).
7	Replication and Policy	Open & Closed	Aggregated data and the results of the analysis will be open; data

No	Data	Availability	Notes
			sources (e.g. interviews and information from confidential/ non-open documents) will be restricted to Partners. Processed data from the EU Policy Roundtable will be made available through the respective deliverable.
8	Monitoring and assessment of the dissemination and communication activities and results	Open & Closed	Website analytics-closed: Available only to the consortium and the European Commission/HaDEA. Nevertheless, KPIs summarising this data will be included in FIERCE's public deliverables. Social media statistics-closed: Available only to the consortium and the European Commission/HaDEA. Nevertheless, KPIs summarising this data will be included in FIERCE's public deliverables. Newsletter subscriptions-closed: Available only to the consortium and the European Commission/HaDEA. Nevertheless, KPIs summarising this data will be included in FIERCE's public deliverables. Data collected from events-restricted: Shared potentially with event participants (anonymised in any case).

It is important to note that all personal data collected / generated will be considered as closed data prior to their anonymisation and aggregation to safeguard the confidentiality of the data subjects

Data accessibility and availability

Public access to the open data will be made available through Zenodo, which will automatically link to OpenAIRE. The data will be fully accessible thanks to the included metadata and the search facility available on Zenodo. At the same time, closed data are intended to be stored and shared amongst

authorised members of the consortium through cloud storage and file sharing providers (e.g. Google Drive).

The following table presents where data will be made accessible in the context of FIERCE.

Table 7:Data accessibility

No	Data	Accessibility
1	State-of-play of downstream space applications	The aggregated, anonymised data will be made available in Zenodo's repository and FIERCE website through D1.1
2	Studying the potential of non-space SMEs to integrate downstream space	The aggregated, anonymised data will be made available in Zenodo's repository and FIERCE website through D1.1 The raw data are already open in Zenodo
3	Profiling the innovation ecosystems	The aggregated, anonymised data will be made available in Zenodo's repository and FIERCE website through D1.2
4	Design Sprint	The aggregated, anonymised data will be made available in Zenodo's repository and FIERCE website through D1.3
5	Development and utilisation of FIERCE digital toolbox	Some aggregated, anonymised data will be made available in Zenodo's repository and FIERCE website through D2.1 and D5.1.

No	Data	Accessibility
		The application forms will remain closed under the storage of OnePass. The input in the self-assessment tool will remain closed within the involved partners' repositories and Tally platform.
6	Delivery and fine-tuning of the FIERCE support programs (Advisory Services, Transformation Projects, Ecosystem Building program)	Cloud storage and partners' organisations repositories (only available to the EC – since the respective deliverables are "Sensitive")
7	Replication and Policy	The aggregated, anonymised data will be made available in Zenodo's repository and FIERCE website through D5.3 as well as through the material of the Replication and Policy Toolkit.
8	Monitoring and assessment of the dissemination and communication activities and results	Cloud storage. Some aggregated data will be made available through the corresponding deliverables on FIERCE website and Zenodo.

Restrictions on use

By utilising Zenodo for sharing the project's openly available data, FIERCE can apply different levels of accessibility for this data taking into account any relevant issues (such as ethical, rules of personal data, intellectual property, commercial, privacy-related, security-related, etc.).

More specifically, Zenodo offers the following levels of data accessibility:

- Open access: Data remains available for re-use. Nevertheless, the level in which this data can be re-used is determined also by their accompanied licence for re-use (see subsection 3.4.1).
- Embargoed status: Access to the data will be restricted until the end of the embargo period, at which time, the content will automatically become publicly available.
- Restricted access: The data will not be made publicly available, and sharing will be made possible only by the approval of the project partner that has the responsibility of the data.
- Closed access: The data is protected against unauthorised access at all levels and only members of the consortium have the right to access it.

Project partners will mainly use the open access level to disseminate the project's data amongst the interested stakeholders. Nevertheless, in some cases embargo periods or restricted access may be used as described in Subsection 3.2.1.

Moreover, FIERCE will ensure open access to all peer-reviewed scientific publications that will be produced in the framework of the project. In particular, according to the Grant Agreement, (ANNEX 5 Specific Rules, Art 17 Open Science) FIERCE will:

- At the latest at the time of publication, deposit a machine-readable electronic copy of the published version or final peer-reviewed manuscript accepted for publication in a trusted repository for scientific publications.
- Ensure immediate open access to the deposited publication — via the repository — under the latest available version of the Creative Commons Attribution International Public Licence (CC BY) or a licence with equivalent rights. Moreover, for monographs and other long-text formats, the licence may exclude commercial uses and derivative works (e.g. CC BY-NC, CC-BY-ND).
- Ensure information is given – via the repository – about any research output or any other tools and instruments needed to validate the conclusions of the scientific publication.

Beneficiaries (or authors) must retain sufficient intellectual property rights to comply with the open access requirements.

Identity ascertainment and data access committee

The identity of stakeholders who want to access the data on Zenodo is not necessary to be ascertained, as the uploaded on Zenodo data are publicly open and no authorisation is needed. On the other hand, closed for the public data will be available only to authorised consortium partners through dedicated mechanisms provided by the cloud storage service employed by the respective partners in order to deposit the data.

The need for a data access committee to evaluate or approve access requests to personal data, is not foreseen because only authorised partners will have access to the project's closed data, accessible only by using their credentials (username/password), and no third-party will re-use them for their benefit.

3.2.3 Metadata

Availability and licences

Metadata of deposited publications generated in the context of FIERCE will be open under a Creative Common Public Domain Dedication (CC 0) or equivalent, in line with the FAIR principles for data

management adopted by the project (in particular machine-actionable). Such metadata will provide information, at least, about the following:

- The publication at hand (author(s), title, date of publication, publication venue);
- Reference to the Horizon Europe funding;
- The name of the project, including its acronym and Grant Agreement number;
- Any particular licensing terms which may apply (depending on the chose license);
- Persistent identifiers that have been attributed to the publication;
- Authors involved in the action, their organisations and the project itself.

Where applicable, the metadata will also include persistent identifiers for any research output or any other tools and instruments needed to validate the conclusions of the publication. The metadata will be available through Zenodo. It is quite unlikely that Zenodo will terminate its operation and stop providing its services, but in such a case all data, metadata, code and documentation uploaded will be transferred and hosted to other suitable repositories without undue delay. In this respect, it is important to note that, since all of FIERCE openly available data will make use of PIDs (i.e., DOIs), which is further elaborated in subsection 3.1.1, the links to the data will not be affected. In parallel, the project's data that will not be openly available for sharing will be deposited, together with their accompanying metadata, code and documentation (if necessary), to the cloud web storage service employed by the project.

Methods, software tools and documentation to access the data

FIERCE emphasises the accessibility of the data collected / generated during the project. With that in mind, no specialised method, software tool and / or documentation is expected to be needed at the moment, in order to access the data. Stakeholders will have the ability to access the data by simply using their web browser (e.g. Mozilla, Google Chrome, Internet Explorer, Safari, etc.) through their computers (either desktop or laptop), smart phones and/ or tablets.

More specifically, they first need to access Zenodo through its webpage (following the link https://zenodo.org/) and utilise the search engine of the repository to search for interesting data. By typing the name of the project the search engine will direct the user to the project's data, ready to be explored and re-used. Moreover, since the data will be available in open formats, we will be ensuring that they can appropriately be read by a range of different software that are widely and freely accessible to all potential users of the data.

Closed data will only be accessed by authorised project partners through usage of a cloud storage service. Again, no specialised method, software tool and / or documentation is needed to this end.

Along these lines, this section has provided the methodology applied in the frame of FIERCE to ensure that its data is as openly accessible as possible by any stakeholder that may find it interesting for re-use. In this context, FIERCE also focuses on providing metadata standards and appropriate metadata vocabularies to increase data interoperability. The following section provides further details in this respect.

3.3 Making data interoperable

Data interoperability refers to the ability of systems and services that create, exchange and use data to have clear, shared expectations for the contents, context and meaning of that data[23]. With that in mind, FIERCE has adopted in its data management methodology the use of metadata vocabularies, standards and methods that will increase the interoperability of the data collected/generated through its activities.

More specifically, the interoperability of the data that will not be publicly shared will be facilitated by the use of the Dublin Core Metadata standard. This standard is a small "metadata element set" which accounts for issues that must be resolved in order to ensure that data meet traditional standards for quality and consistency, while still remaining broadly interoperable with other data sources in the linked data environment. The fifteen elements of the standard provide a vocabulary of concepts with natural-language definitions (e.g. title, creator, author, etc.) that are instantly converted into open machine-readable formats (such as XML, HTML, etc.), enabling machine-processability. Each element is optional and may be repeated, while the standard itself offers ways for refining them, encouraging the use of encoding and vocabulary schemes. The vocabulary of the Dublin Core Metadata standard is presented by the following table[24]:

Table 8: Dublin core Metadata standard vocabulary

No	Element	Element definition
1	Title	A name given to the resource.
2	Creator	An entity primarily responsible for making the content of the resource.
3	Subject	The topic of the content of the resource.
4	Description	An account of the content of the resource.
5	Publisher	An entity responsible for making the resource available.
6	Contributor	An entity responsible for making contributions to the content of the resource.
7	Date	A date associated with an event in the life cycle of the resource
8	Type	The nature or genre of the content of the resource.
9	Format	The physical or digital manifestation of the resource.

[23] L. Steele & T. Orrell (2017). The frontiers of data interoperability for sustainable development. Publish What You Fund and Development Initiatives

[24] Sugimoto, S., Baker, T., & Weibel, S. L. (2002). Dublin Core: Process and Principles. Lecture Notes in Computer Science Digital Libraries: People, Knowledge, and Technology, 25-35.

No	Element	Element definition
10	Identifier	An unambiguous reference to the resource within a given context.
11	Source	A reference to a resource from which the present resource is derived.
12	Language	A language of the intellectual content of the resource.
13	Relation	A reference to a related resource.
14	Coverage	The extent or scope of the content of the resource.
15	Rights	Information about rights held in and over the resource.

Along similar lines, the interoperability of openly available data will be facilitated through Zenodo, since its metadata will be stored internally in JSON format according to a defined JSON schema. This encloses HTML microdata that allows machine-readable data to be embedded in HTML documents in the form of nested groups of name-value pairs. Moreover, the JSON schema provides a collection of shared vocabularies in microdata format that can be used to mark-up pages in ways that can be understood by the major search engines.

FIERCE's data will offer qualified references to other data. A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. Our goal is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data, balanced against the time/energy involved in making a good data model. To be more concrete, our references will specify if one dataset builds on another data set, if additional datasets are needed to complete the data, or if complementary information is stored in a different dataset. The links between the datasets will also be described and, all datasets will be properly cited, including their persistent identifiers.

3.4 Increase data re-use

3.4.1 Documentation for validating data analysis and facilitating data re-use

By utilising Zenodo for sharing the project's openly available data, FIERCE ensures the facilitation of data access, validation and re-use, in compliance to the general policies of Zenodo regarding content, access and reuse. More specifically, the following principles are followed by Zenodo to make data re-useable according to the FAIR principles[25]:

[25] Retrieved from: https://about.zenodo.org/principles/

- R1: (meta)data are richly described with a plurality of accurate and relevant attributes

Each record contains a minimum of DataCite's mandatory terms, with optionally additional DataCite recommended terms and Zenodo's enrichments.

- R1.1: (meta)data are released with a clear and accessible data usage license
- License is one of the mandatory terms in Zenodo's metadata and is referring to an Open Definition license. Data downloaded by the users is subject to the license specified in the metadata by the uploader.
- R1.2: (meta)data are associated with detailed provenance

All data and metadata uploaded is traceable to a registered Zenodo user. Metadata can optionally describe the original authors of the published work.

- R1.3: (meta)data meet domain-relevant community standards

Zenodo is not a domain-specific repository, yet through compliance with DataCite's Metadata Schema, metadata meets one of the broadest cross-domain standards available.

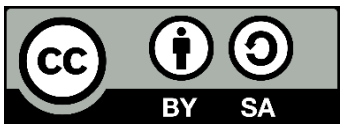
3.4.2 License schemes to permit the widest use possible

The application of a licence to FIERCE's open data is a simple way to ensure that any interested third-party can re-use it. In this context, licences are the instrument which permit a third-party to copy, distribute, display and/or modify the project's data only for the purposes that are set by the licence. Licences typically grant permissions on condition that certain terms are met. While the precise details vary, three conditions are commonly found in licences which are the attribution, non-derivative, and non-commerciality.

Along these lines, FIERCE publishes openly available data under the Creative Commons licencing scheme to foster their re-use and build an equitable and accessible environment for them. Zenodo provides FIERCE the opportunity to publish its open data under 5 Creative Common licences as follows:

- Creative commons Attribution-Share Alike 4.0 (CC BY-SA 4.0) according to which any third party can freely copy, distribute, display and modify the datasets for any purpose. Remix, transform, or built upon data, must be distributed under the same license as the original. Third parties must give appropriate credit, provide a link to the license, and indicate if changes were made.

Figure 2: CC BY-SA 4.0

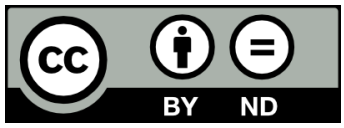


- Creative Commons Attribution 4.0 International (CC BY 4.0) according to which any third party can freely copy, distribute, display and modify the datasets for any purpose. Third parties must give appropriate credit, provide a link to the license, and indicate if changes were made.

Figure 3: CC BY 4.0

- Creative Commons Attribution-No Derivatives 4.0 International (CC BY-ND 4.0) during which any third party can freely copy, distribute, display and modify the datasets for any purpose. Remix, transform, or built upon data, however must not be

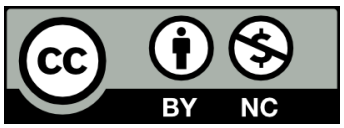
Figure 4: CC BY-ND 4.0



distributed. Third parties must give appropriate credit, provide a link to the license, and indicate if changes were made.

- Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) based on which third parties can copy, distribute, display and modify the datasets for any purpose other than commercial unless they get a permission by project partners first. Third parties must give appropriate credit, provide a link to the license, and indicate if changes were made.

Figure 5: CC BY-NC 4.0



- Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) according to which third parties can copy, distribute, display and modify the datasets for any purpose other than commercial unless they get a permission by project partners first. Remix, transform, or built upon data, however, must not be distributed. Third parties must give appropriate credit, provide a link to the license, and indicate if changes were made.

Figure 6: CC BY-NC-ND 4.0

Different licensing schemes may be selected to better fit the need of FIERCE's open data ensuring not only their long-term preservation and re-use but also the interests of the consortium along with the rights of individuals for whom the data is about. In such a case, this subsection of the DMP will be updated accordingly.

3.4.3 Availability for re-use

The re-use of data is a key component of FIERCE's methodology for making data FAIR. In fact, making data available for re-use ensures interested stakeholders, other than project partners, can benefit from this data, contributing towards maximising the impact of the project. Rich metadata created based on metadata standards that enable proper discovery as well as appropriate licensing schemes facilitate the re-use of FIERCE's open data, allowing them to find valuable utility.

In principle, it is expected that the open data will become available for re-use no later than 120 days after the end of its processing in the framework of the project (i.e. collection, anonymisation, aggregation, etc.) to ensure that any additional data management activities required to this end do not compete with the timely delivery of the project's planned outputs.

With that in mind, the expected time that FIERCE's data will be made openly accessible and uploaded to Zenodo is indicatively provided in the following table:

Table 9: Expected time that data will be made open through Zenodo[26]

No	Data	Expected time for making data open	Notes
1	State-of-play of downstream space applications	30/7/2026	After D1.1 has been accepted by the EC following the 1st Periodic Review.
2	Studying the potential of non-space SMEs to integrate downstream space	30/7/2026	After D1.1 has been accepted by the EC following the 1st Periodic Review. The raw dataset was made available on Zenodo at 26/5/2025
3	Profiling the innovation ecosystems	30/7/2026	After D1.2 has been accepted by the EC following the 1st Periodic Review.
4	Design Sprint	30/7/2026	After D1.3 has been accepted by the EC following the 1st Periodic Review.
5	Development and utilization of FIERCE digital toolbox	30/7/2026 30/12/2027	After D2.1 and D5.1 has been accepted by the EC following the 1st and 2nd Periodic Review.
6	Replication and Policy	30/11/2027	The aggregated analysed data will be made available right away in the Replication and Policy Toolkit (FIERCE website). Afterwards, they will be

[26] This timetable is based on expectations and may be modified during the course of the project taking into account any unforeseen risk that may occur.

No	Data	Expected time for making data open	Notes
			uploaded on Zenodo and FIERCE website after D5.3 been accepted by the EC following the 2nd Periodic Review.
7	Monitoring and assessment of the dissemination and communication activities and results	30/7/2026 30/12/2027	Aggregated data will be available when the corresponding deliverables have been accepted by the EC following the Periodic Reviews.

3.4.4 Data provenance

Data provenance is the documentation of where a piece of data comes from and the processes and methodology by which it was produced. Put simply, provenance answers the questions of why and how the data was produced, as well as where, when and by whom[27]. Accurately recording data provenance is a cornerstone of good data management. FIERCE will use specific elements of the Dublin Core Metadata Standards[28] and the W3C Provenance Data Model[29], to generate specific text files (e.g., README) that will accurately capture the history of each data entity throughout its versions (e.g., based on the DOI versioning Zenodo provides)[30].

3.4.5 Data quality assurance processes

Quality Assurance (QA) and Quality Control (QC) activities are an integral part of FIERCE's data management methodology and are implemented prior to the publication of any data to Zenodo, safeguarding the transparency, consistency, comparability, completeness and accuracy of the data.

QA is a planned system of review procedures conducted outside the framework of developing a dataset, by personnel not directly involved in the dataset development process[31]. In the context of FIERCE, it takes the form of peer-reviews of methods and/or data summaries to assess the quality of

[27] Retrieved from: https://ardc.edu.au/resource/data-provenance/
[28] Retrieved from: https://www.dublincore.org/resources/userguide/creating_metadata/
[29] Retrieved from: https://www.w3.org/TR/prov-dm/
[30] Retrieved from: https://help.zenodo.org/
[31] 2006 IPCC Guidelines for National Greenhouse Gas Inventories, Vol. 1 General Guidance and Reporting, CHAPTER 6 Quality Assurance / Quality Control and Verification.

the dataset and identify any need for improvement, ensuring that the dataset correctly incorporates the scientific knowledge and data generated.

QC is defined as a system of checks to assess and maintain the quality of the dataset being compiled[32]. The relevant procedures of FIERCE are designed to provide routine technical checks as they measure and control data consistency, integrity, correctness and completeness as well as identify and address errors and omissions. In this context, QC checks cover everything from data acquisition and handling, application of approved procedures and methods, and documentation. Some of the general quality checks undertaken in the framework of the project include checking (i) for transcription errors in data input; (ii) that scale measures are within the range of acceptable values; and (iii) whether proper naming conventions are used.

[32] 2006 IPCC Guidelines for National Greenhouse Gas Inventories, Vol. 1 General Guidance and Reporting, CHAPTER 6 Quality Assurance / Quality Control and Verification.

4. Allocation of resources

4.1 Estimated costs for making data FAIR

The costs required for making the data collected/ generated during FIERCE activities FAIR are integrated in the budget of the project. With that in mind, the table which follows provides an overview of the estimated costs of making data FAIR as well as their budget source within the framework of FIERCE.

Table 10:Estimated costs for making data FAIR

No	Data Processing / Management Activity	Budget source	Total estimated effort in Person Months[33]	Total estimated cost in Euro[34]
1	Collection	Budget allocated to the WP under which the respective data are processed	24,68	135.476,85 €
2	Documentation	Budget allocated to the WP under which the respective data are processed	6,17	33.869,21 €
3	Storage	Budget allocated to the WP under which the respective data are processed	3,09	16.934,61 €
4	Access and security	Budget allocated to the WP under which the respective data are processed	3,09	16.934,61 €
5	Preservation	Budget allocated to the WP under which the respective data are processed	1,54	8.467,30 €
6	Availability and re-use	Budget allocated to the WP under which the respective data are processed	9,26	50.803,82 €
7	Overall data management	WP7 and WP9	3,95	21.682,88 €

[33] The total estimated effort for each data processing / management activity reflects the cumulative effort for the implementation of the respective activity for all data collected / generated across the different WPs of FIERCE

[34] The total cost of each data processing / management activity is calculated by multiplying the effort estimated for the respective activity with the weighted average cost of a person month in the framework of FIERCE.

Total	**284.169,29 €**

In order to produce the estimations of the costs for making data FAIR in the context of FIERCE, a series of assumptions were made, taking into account the respective guidelines provided by the Research Data Management Support, a multidisciplinary network of data experts within Utrecht University[35], as well as of the UK Data Service and its data management costing tool[36]. With that in mind, the estimated costs for making FIERCE's data FAIR cover data-related activities and resources across the data lifecycle, spanning from collection and documentation through storage and preservation over to sharing and re-use.

In particular, costs for data collection cover activities necessary for acquiring external datasets (if required), gathering/ generating new data, transcribing (if applicable), formatting and organising this data as well as acquiring informed consent from data subjects. This data processing activity reflects the majority of the costs required for making data FAIR as the majority of FIERCE's data constitutes new data collected/generated over the course of the project. At the same time, data documentation costs address the effort required for describing data (e.g., marking data with variable and value labels, code descriptions, etc.) as well as creating well-defined metadata along with a meaningful description of the context and methodology of how data was collected/generated and processed (where necessary).

Costs for data storage include the resources required for ensuring adequate storage space for the data as well as the effort necessary for conducting data back-ups, while data access and security costs encompass costs related to ensuring access to the data as well as for protecting it from unauthorised access or use or from disclosure. Given that the storage of FIERCE's data will not require the procurement of additional space (other than what is already available to project partners) as well as that no special measures or software are required to access and secure the data (other than what is inherently built into the repositories of FIERCE's data), such costs are kept to a minimum.

Data preservation costs, on the other hand, are estimated relatively higher than data storage, access and security costs, as additional effort will be required in several cases in order to convert the collected/generated data from their original form (e.g., physical interview transcripts) to an open and/or machine-readable format suitable for long-term preservation (e.g. to an .xlsx format.). Adequate effort for data availability and re-use costs is also foreseen to safeguard the appropriate digitisation and anonymisation of the data as well as cover any resources required for data sharing and cleaning. Along the same lines, appropriate effort is foreseen for overall data management as

[35] Research Data Management Support. Guides: Costs of data management. Utrecht University. Retrieved from: https://www.uu.nl/en/research/research-data-management/guides/costs-of-data-management

[36] UK Data Service. Costing Data Management. Retrieved from: https://www.ukdataservice.ac.uk/manage-data/plan/costing

well, in order to cover the effort related with the operationalisation of data management in the framework of FIERCE.

Finally, costs for long-term preservation in the framework of FIERCE are assumed to be ineligible, since the open data of the project will be hosted in the repository of Zenodo free of charge.

4.2 Data management responsibilities

For the effective, proper and secure handling of the data collected/generated in the frame of FIERCE, specific data management roles have been established within the data management methodology and procedures of the project. These responsibilities are outlined in this section of the DMP and are as follows.

Project Coordinator (PC): The PC, Q-PLAN, is responsible for overall data management in the framework of FIERCE, including the elaboration of the DMP and its updates (when necessary, along with support of all partners). At the same time, the PC is responsible for the elaboration of proper templates for the Informed Consent Form and the Data Subject Request Form to be appropriately adjusted and utilised by project partners during the relevant activities of the project as well as for drafting the project's Privacy Policy that has been uploaded on the project's website. The PC in collaboration with the relevant project partners (e.g., Task Leaders) will examine if additional specific privacy policies are required for certain project's tasks and will coordinate the elaboration of such privacy policies. Finally, the PC coordinates with Work Package Leaders, Task Leaders and Responsible Partners to determine whether and how the data collected / generated by the project are shared and become available for re-use, contributes to its quality assurance and uploads the project's openly available data to Zenodo.

Work Package Leaders (WPL): The WPL is responsible for coordinating the implementation of the data processing activities performed under the WPs they are leading. Moreover, they align with the PC and the respective Work Task Leader on whether and how the data gathered/produced under the tasks that fall within the WP they are leading will be shared and/or re-used. This includes the definition of access procedures as well as potential embargo periods along with any necessary software and/or other tools which may be required for data sharing and re-use. Finally, the WPL are the main responsible for assuring the quality of the data stemming from the activities of the WP they are leading, including assessing their quality and indicating any need for improvement to the respective Work Task Leaders.

Work Task Leaders (WTL): WTLs are responsible for the data collected / generated in the frame of the tasks that fall under their leadership as well as for safeguarding their appropriate and timely processing. Moreover, they are responsible for properly adjusting the Informed Consent Form and Data Subject Request Form templates, to the needs and specificities of the activities carried out in the task they are leading. WTLs are responsible for identifying the need for a specific privacy policy regarding the task they are leading and collaborate with the PC for drafting and releasing it to the public. Finally, they undertake any necessary actions to prepare the data collected / generated through the tasks they are leading for sharing either within the consortium or openly (including the use of proper naming conventions, application of suitable anonymisation techniques, creation of appropriate metadata and documentation, etc.).

Partners: All project partners are tasked to collect, digitise, anonymise, store, destroy and / or otherwise process data for the specific purpose of the activity in which it has been collected /

generated within the project. They are responsible for appropriately collecting the necessary consent for processing data as well as for ensuring that the Informed Consent Form and the Data Subject Request Form used to this end are properly adjusted to the needs of the activity they are participating (including references to the project's Privacy Policy and any other applicable specific privacy policies) and, in any particularities, applicable to their organisation while ensuring adherence to provisions of relevant national data protection legislation in their respective country. Moreover, they are responsible for managing the consents they have collected with a view to demonstrating their compliance with the relevant applicable EU and national regulation(s). Finally, they perform quality checks to assess and maintain the quality of the dataset(s) held within their records.

Data repositories: Data repositories are tasked with the storage and long-term preservation of the project's data. In this respect, Zenodo will maintain and preserve the openly available data of FIERCE, enabling its sharing and re-use. To this end, Zenodo assigns metadata and DOIs to the data, while also taking all necessary measures to securely back-up the data and restore it, safeguarding its long-term preservation.

In this context, the following table illustrates the allocation of data management responsibilities amongst the members of the FIERCE consortium per data collected/generated under each WP.

Table 11:Data management responsibilities of FIERCES's partner per data collected/generated under each WP

WP	WPL	Data	Tasks	WTL	Responsible Partner
WP1	NVS	State-of-play of downstream space applications	1.1	DREVEN	All partners involved
WP1	NVS	Studying the potential of non-space SMEs to integrate downstream space	1.1	DREVEN	Q-PLAN
WP1	NVS	Profiling the innovation ecosystems	1.2	NVS	All partners involved
WP2	NVS	Design Sprint	1.3	DREVEN	All partners involved
WP2	EMNP	Development and utilization of FIERCE digital toolbox	2.1, 2.2, 3.1, 4.1	EMNP, FBA, DREVEN	EMNP, FBA, DREVEN, Q-PLAN
WP3 and WP4	FBA	Delivery and fine-tuning of the FIERCE support programs (Advisory Services, Transformation Projects, Ecosystem Building program)	3.1, 3.2, 3.3, 4.1, 4.2, 4.3, 2.3, 5.1	FBA, EMNP, NVS, DREVEN	All partners involved
WP5	EMNP	Replication and Policy	5.2, 5.3, 5.4	EMNP, Q-PLAN, NVS	All partners involved
WP6 and WP8	Q-PLAN	Monitoring and assessment of the dissemination and communication activities and results	6.1, 6.3, 8.1, 8.3	Q-PLAN, TTG	All partners involved

5. Data Security

FIERCE will securely handle any collected / generated data throughout its entire lifecycle as it is essential to safeguard this data against accidental loss and / or unauthorised access. To achieve this the project applies appropriate technical and organisational measures based on a risk assessment of the relevant data that takes into account the impact and the likelihood of a potential data breach. With that in mind, the project's data security strategy aims at minimising the probability that a data breach will occur during the course and after the completion of FIERCE, either from human error or hardware failure, as well as inhibit any unauthorised access. Particularly, in case of personal data collection / generation it is crucial that this data can only be accessible by those authorised to do so.

All project partners are responsible for processing[37] data using appropriate means, such as private servers or cloud service providers that adhere to the relevant legal data protection requirements (e.g., GDPR) and will ensure that this data is protected, and any necessary data security controls have been implemented, to minimise the risk of information leak and destruction. This case refers to the data that will be closed and therefore will not be shared and / or re-used within the framework of the project. In this case, to minimise the consequences of potential data losses, the data will be backed up at regular time intervals based on change frequency and criticality. The backed-up files will be stored in appropriate storage media including external hard drives, flash drives, or other reputable cloud services, so as to safeguard their preservation, while also enabling their recovery at any time. Moreover, integrity checks[38] will be carried out regularly ensuring that the stored data has not been changed or corrupted.

Access to closed data will only be permitted to authorised project partners. In case there is a personal data breach, the responsible project partner will notify, without undue delay and, where feasible, not later than 72 hours after having become aware of it, its competent national supervisory authority (e.g., data protection authority) as well as the data subject(s) that may be affected by the breach. Moreover, the responsible partner will document any personal data breaches, including information such as the facts relevant to the breach, its effects and the remedial action(s) taken.

Identification and authentication access controls play an important role in the context of the project, as they help partners to protect the data collected / generated during FIERCE and especially personal data. To this end, each project partner is responsible for and committed to ensuring the application of appropriate access controls to the data they are processing. Additionally, in order to safeguard the privacy of the users of the FIERCE website and the tools it includes dedicated privacy policies will

[37] Processing, according to Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation), means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[38] An integrity check is the process of comparing the current state of stored data and/or programs to a previously recorded state in order to detect any changes.

define the way in which these online spaces collect, process and use personal data, the security procedures followed, the users' rights as well as the cookies policy employed.

On another note, openly available data will be stored safely for long-term preservation on Zenodo, in the same cloud infrastructure as research data from CERN's Large Hadron Collider, using CERN's battle-tested repository software INVENIO, which is used by some of the world's largest repositories (such as INSPIRE HEP and the CERN Document Server). Along these lines, data is stored and backed up in CERN's EOS service in an 18 petabytes disk cluster. Both data files and metadata are kept in multiple online replicas and independent replicas ensuring their long-term preservation as well as their recovery when necessary. Moreover, for each file two independent MD5 checksums are stored. One checksum is stored by INVENIO, used to detect changes to files made from outside of it whereas the other checksum is stored by EOS, and used for automatic detection and recovery of file corruption on disks. In this context, access control is applied by the different level of openness that Zenodo allows (i.e., open, embargoed, restricted and closed).

6. Ethical aspects and other procedures

This chapter addresses the ethical aspects of the FIERCE's Data Management Plan and the ethical compliance of the underlying data foreseen to be collected / generated under the project's activities. The project processes data that is not included in any special category of personal data (i.e., non-sensitive data) according to the relevant data protection legislation (e.g. GDPR). In accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), all personal data processed for project's activities shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes relative to project's objectives and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data.

For all personal data processing activities within the framework of the project at least one lawful basis as of Art. 6 GDPR applies. Where informed consent is chosen as the lawful basis for processing, all relevant provisions of the data protection legislation (e.g., Art.7 GDPR) are observed. Under this light, further details about the scope of the activities that entail data collection/generation in the frame of FIERCE along with the procedures for identifying/recruiting suitable stakeholders to take part in them as well as for obtaining their informed consent are defined by the respective WP Leaders (NVS-DE for WP1, EMNP for WP2, FBA for WP3, FBA for WP4, EMNP for WP5, Q-PLAN for WP6, WP7, WP8, WP9). Moreover, personal data processing carried out by partners are in line with relevant EU and national regulations. The project's templates of the Informed Consent Form and the Data Subject Request Form, used in the implementation of the project's activities, are compliant with the General Data Protection Regulation and annexed to this DMP (see Annexes). Last but not least, no transfer of personal data outside the EU is foreseen as part of the project's implementation. In case of data storage providers situated both inside and outside the EEA, partners are committed to ensure their compliance with the relevant GDPR requirements before start using their services.

As mentioned before, regarding the open calls, data is and will be collected only for the purpose of selection and evaluation. The personal data is collected through the One Pass Platform (https://getonepass.eu/). The data collected is data of the applicant (name and surname), contact data and data that are necessary to assess the potential of the proposal. Sociodemographic indicators such as gender are optionally gathered. We do not collect any sensitive data.

More specifically, data collected through OnePass is managed according to the OnePass Privacy Notice for open call applicants (Privacy notice (open call)).

The applications for the Transformation Projects will be shared also with external experts only for the purpose of their evaluation and after the ratify the Confidentiality Statement and the Non-Conflict of Interest. In addition to the technical evaluation of the Transformation Projects focusing on the scientific merit, the quality of the management and the potential impact, the Ethics assessment is needed to

ensure that all activities carried out under FIERCE Project comply with fundamental ethical principles, taking special attention, in this case, to ethical issues related to space data processing.

FBA, as partner responsible for the FSTP Management, will set up a process to ensure that the projects that are to be funded comply with the ethical standards and guidelines of Horizon Europe by means of the Ethic Assessment of all selected Transformation Projects (see Task 4.2) which will be done by external ethics experts according with the ethical guidelines of Horizon EU. The resulting 'Ethics Summary Report' may lead to include either specific requirements (contractual obligation) in the ethics section of the Sub Grant Agreement [SGA] and/ or countermeasures tackling ethical issues within the Transformation Plans which will be followed up by the Lead Mentors.

7. Conclusions and way forward

This interim version of the FIERCE DMP aims at safeguarding the sound management of the data collected, processed and/or generated during the project's activities across their entire lifecycle, while also making them FAIR. It describes all the underlying processes of the FIERCE data management, collection, process and generation, in accordance with the GDPR guidelines, and sheds light on (i) the data being collected, processed and/or generated under the project activities, (ii) the specific objectives under which each dataset is collected, processed and/or generated, (iii) the allocation of resources and data management responsibilities and (iv) the data security and ethical aspects of the data.

In the framework of FIERCE, the DMP is a living document and is updated throughout the course of the project, considering its latest developments and available results. It is expected to be further developed and updated at least once more at the end the project (i.e., D9.1 in M36). If necessary, additional ad hoc updates may be released in order to include new data, better detail and/or reflect modifications in the methodologies applied or other aspects relevant to data management (such as costs for making data FAIR, size of data, etc.), changes in consortium policies and plans or other potential external factors.

8. Annexes

8.1 Annex I – Informed Consent Form

Text in grey colour contains guidelines for adjusting this template and should be deleted.

Text in grey colour contains examples and should be adjusted to the context of each activity.

Text included in < > and/or should be replaced with content that is suitable to the context of each activity & project as well as to the organisation seeking to obtain the consent.

Before using this template take the time to carefully read and adjust it to the needs of the activity at hand as well as to any relevant regulations and particularities applicable to your country and organisation.

INFORMED CONSENT FORM

Who we are:

We are < Insert Partner Name > and we are contacting you in the framework of FIERCE a project funded by the European Union under the Horizon Europe Framework Programme for Research and Innovation.

Project:

FIERCE – Financing and Innovation Ecosystems for SMEs to innovate for Raw materials and Circular Economy solutions and using downstream space technologies (GA Number 101177496).

Partner:

Organisation name: < Insert Partner Name >

Address: < Insert Partner Address >.

Phone: < Insert Partner Phone >.

E-mail: <Insert Partner Generic E-mail Address >

Responsible persons:

You may delete the line referring to the Data Protection Officer if your organisation does not have one.

#	Role	Name	E-mail

1	FIERCE Project Manager	<Insert name of project manager from your organisation>	<Insert e-mail of project manager from your organisation >
2	Interviewer	<Insert name of interviewer from your organisation >	<Insert e-mail of interviewer from your organisation >
3	Data Protection Officer	<Insert name of DPO from your organisation >	<Insert e-mail of DPO from your organisation >

What do we need from you?

 # Please explain in a brief paragraph the activity and its purpose under the frame of the project.

Example: We need you to participate in an interview that will be carried out by FIERCE with a view to shedding light on the success factors and barriers that you faced in your effort to integrate space-enabled data and/ or services in your business.

The interview is expected to last for no more than < Insert number of minutes > minutes.

 # Please adapt the following text to accurately depict the type of personal data to be collected.

To effectively conduct this interview, we need to process some of your personal data:

- Your contact details (full name, email, phone number);
- Some basic demographics (age, gender);
- Your professional info (organization, job position, field of expertise);
- Your education info
- Your opinions on the subject matter.

Why do we need your data & what will we do with them?

We need your data to contact you in order to plan and carry out the aforementioned interview and to resolve any ambiguities, questions and other issues that may arise after and as a result of the interview. We also need to record your data to keep track of the interview process. The project's deliverables that will be derived by the interview will not include your personal data or any other information that could identify you. Your personal data will remain on our written notes (interview's transcript).

We will share your data with a few other FIERCE project partners that are also involved in this task if needed and will participate in the drafting of the relevant deliverables. We are also obliged to grant access to your data to:

EU officials such as our Project Officer for purposes related to project's evaluation;
EU agencies and other authorities for project's auditing purposes.

We would also be very happy if you gave us your consent to inform you about the project's progress (e.g., by sending you a newsletter or similar messages).

How can you withdraw your consent?

You should know that you can withdraw your consent at any time by communicating either on the phone or by email with the responsible persons listed in the previous page. With regards to the informational messages and newsletters you can always opt out by simply clicking the link "Unsubscribe" or something similar included at the end of all the relevant messages.

I hereby give my consent to the processing of my personal data needed for:

(Please, tick the boxes below to confirm that you give us your consent for the respective subject. Any boxes left unticked mean that ***you do not consent to the relevant subject***.)

#	Consent Subject	Tick box
1	My participation in an interview that will be carried out by FIERCE to < insert key objective of the interview >	
2	Receiving newsletters and messages regarding FIERCE activities	

Name of participant _____ Date _____ Signature _____

8.2 Annex II – Data Subject Request Form

Data Subject Request form

Text in grey colour contains guidelines for adjusting this template and should be deleted.

Text included in < > should be replaced with content that is suitable to the context of each activity & project as well as to the organisation seeking to obtain the consent.

You may delete the data referring to the Data Protection Officer if your organisation does not have one.

CONTACT

<Insert name of responsible Project Manager>	<Insert name of DPO > (Data Protection Officer)

Data Subject Request Form

This form should be used to submit a data subject request under the provisions of the European Union General Data Protection Regulation (GDPR).

Submitter Details

Title:	
Name:	
Address:	

Type of Request

Please select the type of request you are making:

- ☐ Consent withdrawal
- ☐ Access request
- ☐ Rectification of personal data
- ☐ Erasure of personal data
- ☐ Restriction of processing of personal data
- ☐ Personal data portability request
- ☐ Objection to processing of personal data
- ☐ Request regarding automated decision making and profiling

PERSONAL DATA INVOLVED

Request details

REQUEST REASON/JUSTIFICATION

Name: .....

Signature: .....

Date: .....

***

Once completed, this form should be submitted via e-mail to < Insert contact e-mail of Partner > or posted to:

< Insert Partner Name >

<Insert Partner Address>

8.3 Annex III – Record of Processing Activities

No	Project Activity / purpose	Data processing activity	Linked WP(s)	Linked Tasks	Data subjects	Data source	Data category(-ies)	Responsible partner	Involved partner (s)	Type of involvement	Special category (Art. 9 GDPR)	Lawfulness of processing	Transfer to third countries (non EU-EEA)	Recipients	Comments
1	State-of-play of downstream space applications	Interviews	WP1	Task 1.1	Interviewees	Data subject	Contact details Professional information	QPL			No	Art. 6(1)(a) - consent	No		
2	State-of-play of downstream space applications	Interviews	WP1	Task 1.1	Interviewees	Data subject	Contact details Professional information	NVS			No	Art. 6(1)(a) - consent	No		
3	State-of-play of downstream space applications	Interviews	WP1	Task 1.1	Interviewees	Data subject	Contact details Professional information	DREVEN			No	Art. 6(1)(a) - consent	No		
4	State-of-play of downstream space applications	Interviews	WP1	Task 1.1	Interviewees	Data subject	Contact details Professional information	EMNP			No	Art. 6(1)(a) - consent	No		
5	State-of-play of downstream space applications	Interviews	WP1	Task 1.1	Interviewees	Data subject	Contact details Professional information	TTG			No	Art. 6(1)(a) - consent	No		
6	State-of-play of downstream space applications	Interviews	WP1	Task 1.1	Interviewees	Data subject	Contact details Professional information	EIT-RM			No	Art. 6(1)(a) - consent	No		
7	State-of-play of downstream space applications	Interviews	WP1	Task 1.1	Interviewees	Data subject	Contact details Professional information	FBA			No	Art. 6(1)(a) - consent	No		

8	Studying the potential of non-space SMEs to integrate downstream space	Survey	WP1	Task 1.1	Survey participants	Data subject	Contact details Professional information	Q-PLAN							
9	Analysis of ideas from the Design Sprint	Event organisation	WP1	Task 1.3	Event participants	Data subject	Contact details Professional information Videos and photos	DREVEN			No	Art. 6(1)(a) - consent	No		
10	Analysis of ideas from the Design Sprint	Event organisation	WP1	Task 1.3	Event participants	Data subject	Contact details Professional information Videos and photos	Q-PLAN			No	Art. 6(1)(a) - consent	No		
11	Analysis of ideas from the Design Sprint	Event organisation	WP1	Task 1.3	Event participants	Data subject	Contact details Professional information Videos and photos	NVS			No	Art. 6(1)(a) - consent	No		
12	Analysis of ideas from the Design Sprint	Event organisation	WP1	Task 1.3	Event participants	Data subject	Contact details Professional information Videos and photos	FBA			No	Art. 6(1)(a) - consent	No		
13	Analysis of ideas from the Design Sprint	Event organisation	WP1	Task 1.3	Event participants	Data subject	Contact details Professional information Videos and photos	TTG			No	Art. 6(1)(a) - consent	No		
14	Analysis of ideas from the Design Sprint	Event organisation	WP1	Task 1.3	Event participants	Data subject	Contact details Professional information Videos and photos	EMNP			No	Art. 6(1)(a) - consent	No		
15	Analysis of ideas from the Design Sprint	Event organisation	WP1	Task 1.3	Event participants	Data subject	Contact details Professional information Videos and photos	EIT-RM			No	Art. 6(1)(a) - consent	No		
16	Deployment and utilisation of the FIERCE digital toolbox	Use of FIERCE digital toolbox	WP2	Task 2.2	FIERCE digital toolbox users	Data subject	Contact details Professional information	FBA			No	Art. 6(1)(a) - consent	No		

							Open call applications Inputs to the self-assessment tool								
17	Deployment and utilisation of the FIERCE digital toolbox	Use of FIERCE digital toolbox	WP2	Task 2.2	FIERCE digital toolbox users	Data subject	Contact details Professional information Open call applications Inputs to the self-assessment tool	EMNP			No	Art. 6(1)(a) - consent	No		
18	Delivery, monitoring and fine tuning of the FIERCE support programs	Applications, provision of services, feedback forms	WP3 and WP4	Task 3.1-4.1, Task 3.2-4.1, Task 3.3-4.3,	Support Programs beneficiaries	Data subject	Contact details Professional information	FBA			No	Art. 6(1)(a) - consent	No		
19	Delivery, monitoring and fine tuning of the FIERCE support programs	Applications, provision of services, feedback forms	WP3 and WP4	Task 3.1-4.1, Task 3.2-4.1, Task 3.3-4.3, Task 2.1-5.1,	Support Programs beneficiaries	Data subject	Contact details Professional information	Q-PLAN			No	Art. 6(1)(a) - consent	No		
20	Delivery, monitoring and fine tuning of the FIERCE support programs	Applications, provision of services, feedback forms	WP3 and WP4	Task 3.1-4.1, Task 3.2-4.1, Task 3.3-4.3, Task 2.1-5.1,	Support Programs beneficiaries	Data subject	Contact details Professional information	NVS			No	Art. 6(1)(a) - consent	No		

21	Delivery, monitoring and fine tuning of the FIERCE support programs	Applications, provision of services, feedback forms	WP3 and WP4	Task 3.1-4.1, Task 3.2-4.1, Task 3.3-4.3, Task 2.1-5.1,	Support Programs beneficiaries	Data subject	Contact details Professional information	EIT-RM			No	Art. 6(1)(a) - consent	No		
22	Delivery, monitoring and fine tuning of the FIERCE support programs	Applications, provision of services, feedback forms	WP3 and WP4	Task 3.1-4.1, Task 3.2-4.1, Task 3.3-4.3, Task 2.1-5.1,	Support Programs beneficiaries	Data subject	Contact details Professional information	EMNP			No	Art. 6(1)(a) - consent	No		
23	Delivery, monitoring and fine tuning of the FIERCE support programs	Applications, provision of services, feedback forms	WP3 and WP4	Task 3.1-4.1, Task 3.2-4.1, Task 3.3-4.3, Task 2.1-5.1,	Support Programs beneficiaries	Data subject	Contact details Professional information	TTG			No	Art. 6(1)(a) - consent	No		
24	Delivery, monitoring and fine tuning of the FIERCE support programs	Applications, provision of services, feedback forms	WP3 and WP4	Task 3.1-4.1, Task 3.2-4.1, Task 3.3-4.3, Task 2.1-5.1, 5.2	Support Programs beneficiaries	Data subject	Contact details Professional information	DREVEN			No	Art. 6(1)(a) - consent	No		

25	Replication and Policy activities	Interviews	WP5	Task 5.3	Interviewees	Data subject	Contact details Professional information	Q-PLAN			No	Art. 6(1)(a) - consent	No		
26	Replication and Policy activities	EU policy roundtable	WP5	Task 5.4	Event participans	Data subject	Contact details Professional information Photos	NVS			No	Art. 6(1)(a) - consent	No		
27	Monitoring and assessment of the dissemination and communication activities	Social media analytics	WP6 and 8	Task 6.1, Task 8.1	Social media followers	Data subject	Likes, follows, posts, impressions, people reached	Q-PLAN			No	Art. 6(1)(a) - consent	No		
29	Monitoring and assessment of the dissemination and communication activities	Newsletter subscriptions	WP6 and 8	Task 6.1, Task 8.1	Newsletter subscribers	Data subject	Contact details	Q-PLAN			No	Art. 6(1)(a) - consent	No		
30	Monitoring and assessment of the dissemination and communication activities	Event organization (e.g. Info days, final event, roadshows etc.)	WP6 and 8	Task 3.1,3.2 3.3,4.1 4.2,4.3 6.1,6.3 8.1,8.3	Event participans	Data subject	Contact details Professional information Photos	Q-PLAN			No	Art. 6(1)(a) - consent	No		
31	Monitoring and assessment of the dissemination and communication activities	Event organization (e.g. Info days, final event, roadshows etc.)	WP6 and 8	Task 3.1,3.2 3.3,4.1 4.2,4.3 6.1,6.3 8.1,8.3	Event participans	Data subject	Contact details Professional information Photos	TTG			No	Art. 6(1)(a) - consent	No		
32	Monitoring and assessment of the dissemination and communication activities	Event organization (e.g. Info days, final event, roadshows etc.)	WP6 and 8	Task 3.1,3.2 3.3,4.1 4.2,4.3 6.1,6.3 8.1,8.3	Event participans	Data subject	Contact details Professional information Photos	FBA			No	Art. 6(1)(a) - consent	No		
33	Project management, meetings and reporting	Project management	WP7, WP9	All tasks within	Project partners	Data subject	Contact details Professional information Videos and photos	Q-PLAN			No	Art. 6(1)(b) - contract	No		

34	Project management, meetings and reporting	Project management	WP7, WP9	All tasks within	Project partners	Data subject	Contact details Professional information Videos and photos	NVS			No	Art. 6(1)(b) - contract	No		
35	Project management, meetings and reporting	Project management	WP7, WP9	All tasks within	Project partners	Data subject	Contact details Professional information Videos and photos	FBA			No	Art. 6(1)(b) - contract	No		
36	Project management, meetings and reporting	Project management	WP7, WP9	All tasks within	Project partners	Data subject	Contact details Professional information Videos and photos	DREVEN			No	Art. 6(1)(b) - contract	No		
37	Project management, meetings and reporting	Project management	WP7, WP9	All tasks within	Project partners	Data subject	Contact details Professional information Videos and photos	TTG			No	Art. 6(1)(b) - contract	No		
38	Project management, meetings and reporting	Project management	WP7, WP9	All tasks within	Project partners	Data subject	Contact details Professional information Videos and photos	EMNP			No	Art. 6(1)(b) - contract	No		
39	Project management, meetings and reporting	Project management	WP7, WP9	All tasks within	Project partners	Data subject	Contact details Professional information Videos and photos	EIT-RM			No	Art. 6(1)(b) - contract	No		

FiERCE
MAKING SPACE FOR GREEN SOLUTIONS

GA 101177496

Partners

Q-PLAN INTERNATIONAL

NOVASPACE

FundingBox

europa media

TechTour

eit RawMaterials Connecting matters

DREVEN

@fierce-project

Funded by the European Union under GA no. 101177496. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

Funded by the European Union