



CIRAN

D1.3.

Data Management Plan



Views and opinions expressed are 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

Disclaimer

This information and content of this report is the sole responsibility of the CIRAN consortium members and does not necessarily represent the views expressed by the European Commission or its services. Whilst the information contained in the documents and webpages of the project is believed to be accurate, the author(s) or any other participant in the CIRAN consortium makes no warranty of any kind with regard to this material.

Report Information

Grant Agreement / Proposal ID	101091483
Project Title	Critical RAW materials extraction in environmentally protected areas
Project Acronym	CIRAN
Project Coordinator	International Raw Materials Observatory
Project starting date / end date	January 2023 / December 2025
Related Work Package	WP 1
Lead Organisation	International Raw Materials Observatory
Document title	Data Management Plan
Submission Date	24 April 2023
Dissemination level	Public

How to Cite

Correia, C., Falck., W.E. (2023). Data Management Plan. Deliverable 1.3 of the Critical raw materials extraction in environmentally protected areas (CIRAN) project. Grant Agreement No. 101091483 of the European Union's Horizon Europe research and innovation programme.

Quality Verification

Prepared by	Checked by	Verified by	Approved by
Vitor Correia	Eberhard Falck	Ronald Arvidsson	Vitor Correia

Revision History

Revision	Revision Date	Changes	Authorised	Function
1	20/04/2023	Wording adjustments	Eberhard Falck	President
2	24/04/2023	Adjustments on treatment of personal and sensitive information	Eberhard Falck	President

Executive Summary

This Data Management Plan (DMP) sets the framework for the responsible handling of data collected and/or generated by the Horizon Europe project CIRAN. While the Grant Agreement and Ethics Guidelines establish rules and principles that must guide the Consortium in the implementation of CIRAN, the DMP provides detailed guidelines for dealing with the different types of generated data.

The DMP includes procedures for data collection, documentation, storage, backup, and preservation, as well as guidelines for data sharing, data access, and data reuse. Moreover, it establishes clear roles and responsibilities for all stakeholders involved in data generation and management.

The procedures set forth in the DMP are intended to complement the Grant Agreement and the CIRAN Ethics Guidelines, and to provide additional clarity and guidance on the management of data generated and/or handled by the project. By adhering to these guidelines, CIRAN ensures that it remains accountable to the individuals and communities involved in its activities, while also upholding its responsibility as a recipient of public funding to ensure that data are managed in accordance with the highest standards of data protection and privacy.

In the event of any conflicts, the Grant Agreement shall serve as the guiding document, and the DMP shall be interpreted in a manner consistent with the Grant Agreement.

Table of Contents

1	Introduction	3
2	Legal Background	4
3	Data Management	5
3.1	Types of Data	5
3.2	Standards for Data Management	5
3.2.1	Storage	5
3.2.2	Preservation and Backup.....	5
3.2.3	File Formats	6
3.2.4	Document Naming and Coding	6
3.2.5	Data Sharing	7
3.3	Management of Sensitive Data	7
3.3.1	Identification of Sensitive Data	7
3.3.2	Keeping Personal Data Private and Anonymisation	7
3.3.3	Aggregation of Data.....	8
3.3.4	Informed Consent.....	8
3.3.5	Sharing of Data Among the Consortium.....	8
3.3.6	Holding Times of Sensitive Data	8
3.3.7	Accessibility of Sensitive Data by Persons Concerned	8
3.4	Management of Public Data	9
3.4.1	Making Data Findable.....	9
3.4.2	Making Data Accessible.....	9
3.4.3	Making Data Interoperable	9
3.4.4	Making Data Re-Usable	10
4	Conclusions	11
5	Bibliography	12

1 Introduction

CIRAN is a Horizon Europe Coordination and Support Action (CSA) project that aims at developing, testing, and validating processes to arrive at systemic policy-making, while balancing environmental protection and societal needs for accessing critical raw materials (CRMs). The project proposes a logical framework to validate extraction on the basis of a system-oriented assessment and the co-creation of knowledge (i.e. tested and validated by communities located in or nearby environmentally protected areas). It aims at creating novel social contract models, identifying the rights, obligations and responsibilities of governments (national/regional), communities and mine operators, capable of dealing with transformations and challenges due to climate change.

Given the project's multifaceted activities that involve various stakeholders and the collection of primary and secondary data, the establishment of rules to protect sensitive data and intellectual property rights is crucial. This Data Management Plan (DMP) defines how CIRAN's research data will be managed during and beyond the lifetime of the project, emphasising the importance of open and transparent data sharing, while also recognising the need to protect sensitive data and intellectual property rights. It includes procedures for data collection, documentation, storage, backup, and preservation, as well as guidelines for data sharing, data access, and data reuse and roles and responsibilities for all stakeholders involved in data generation and management.

By implementing the procedures outlined in this DMP, CIRAN safeguards sensitive data, ensures accountability and transparency in data management and enables Consortium partners to access and utilise data in a manner that respects privacy, security, and ethical considerations.

2 Legal Background

Article 8 of the EU Charter of Fundamental Rights (The European Union, 2012) explicitly states that EU citizens have the right to the protection of their personal data. This fundamental right is enshrined in the European Union General Data Protection Regulation (GDPR) laid out in 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 (European Commission, 2016). In addition, the CIRAN Grant Agreement, which has been signed by all Consortium Partners, provides further guidance on ethical practices, data protection and respect of intellectual property rights (IPR). Specifically, Article 13 of Regulation (EU) 2016/679 defines rules for handling sensitive and classified information, Article 14 mandates compliance with ethical principles and the respect of national, EU, and international laws, Article 15 imposes a commitment to data protection, and Article 16 sets the rules for the protection of intellectual property rights.

Hence, the CIRAN DMP abides to four relevant legal frameworks:

- Compliance with the GDPR on the collection, storage and processing of personal data.
- IPR applicable to the data generated and to the protection of intellectual property.
- National Laws: CIRAN's researchers consider any national laws that may apply to the data they generate, including laws on privacy, data protection, and intellectual property.
- Horizon Europe Grant Agreement: Consortium partners comply with the terms and conditions of the CIRAN Grant Agreement, which is aligned with the rules and requirements for EU-funded research projects.

In addition to these legal frameworks, the CIRAN project has a strong commitment to upholding the ethical principles established in Deliverable 1.2 (Ethics Guidelines), that describes the ethical considerations that guide CIRAN's research and practices, including informed consent, data anonymisation and secure data storage and sharing.

3 Data Management

The purpose of these guidelines is to ensure compliance with the legal background mentioned above, and to guarantee that the best practices are put in place for achieving the dissemination goals predefined in CIRAN's Grant Agreement, while protecting sensitive data.

The different types of data are described below (primary/ secondary), and the standards put in place for its management are also explained. A distinction between public and sensitive data is made, and the practices used for their treatment are listed.

3.1 Types of Data

CIRAN's data collection efforts will involve both secondary and primary sources. Secondary data will be gathered through desk research, while primary data will be derived from interviews and public consultations, that will result in knowledge co-creation.

The use of existing (secondary) data will respect ethical guidelines, to ensure that copyright and Intellectual Property Rights are respected. For the case of primary data, the focus is on ensuring that the privacy of contributors is safeguarded, and that proper consent is obtained before the data are shared or published in any way.

The combination of primary and secondary data will support the achievement of CIRAN's aim, which is to develop, test and validate processes to arrive at systemic policymaking, balancing environmental protection and societal needs for accessing critical raw materials (CRMs).

3.2 Standards for Data Management

Standardization helps to ensure compliance with the existing legislative background and enables effective data sharing and collaboration. Defining standards for data management is therefore critical to ensure that the project's data are effectively managed, preserved, and shared with others. These concern document storage, preservation and backup, accepted files format, document naming and coding.

3.2.1 Storage

Establishing standards for document storage requires organising data in a logical and consistent manner to ensure a common understanding of file organisation, which facilitates access to data. The following has been established:

All documents produced by the project will be stored and archived in SharePoint (provided by MS Teams). It was selected as the Platform for document storage because it is a secure, intuitive Platform that allows all partners to access and upload project documentation. A common folder "Repository" has been created for sharing information relevant to Consortium members. It includes separate folders for communication; contacts; deliverables; finances; meetings; official documents and templates. Separate folders for WP ongoing discussions were also created. For detailed information on the use of CIRAN's SharePoint repository please revert to Deliverable 1.1 Project Management Plan.

The project thus relies on the data protection put into place by Microsoft for 'cloud'-services. However, the project has no control over the location of the respective servers.

3.2.2 Preservation and Backup

CIRAN recognises the importance of ensuring that data are not lost over time and remains accessible and usable in the future. As such, managing data is a critical aspect of CIRAN's operations. To ensure data

preservation, Consortium partners are required to upload backup versions of all documents they create onto the SharePoint Platform. Furthermore, working files that contain primary and derived data shall be uploaded weekly, while draft reports shall be uploaded monthly to the platform. This approach guarantees the availability of crucial data for future reference and promotes the continuity of CIRAN's activities.

Moreover, it is mandatory for a backup version to be uploaded to the SharePoint Platform when a responsible party sends a deliverable or report to a reviewer, as well as when the final deliverable or report is produced. Therefore, when the Project Coordinator uploads a deliverable on the EU's Platform, the partner responsible for that deliverable shall also upload it on the SharePoint Platform. This ensures that a backup copy of the deliverable is available in case the original is lost or becomes inaccessible.

Once deliverables are approved by the European Commission, the Project Coordinator will copy them to Zenodo, an open-access platform that provides secure archiving and preservation of research data. Zenodo is operated by OpenAIRE, a European infrastructure that supports open access to research data, and is supported by CERN, the European Organisation for Nuclear Research.

In summary, ensuring the preservation and accessibility of data is a fundamental component of CIRAN's management. Consortium partners must upload backup versions of their documents to the SharePoint Platform, and approved deliverables are copied to Zenodo by the Project Coordinator. These measures safeguard against data loss and ensure that the data produced by CIRAN remains available for future use.

3.2.3 File Formats

File format and compatibility are essential for ensuring accessibility and fluidity on exchanging documents between different partners using different systems. It also foresees the preservation of data, to ensure that it can be archived and retrieved in the future.

Standardisation here ensures that documents can be easily shared, reused and preserved over time. The following file formats shall be used:

- Word processor documents – Microsoft Office WORD version 2003 or higher (.doc, .docx, or .odt formats);
- Spreadsheet documents – Microsoft Office EXCEL version 2003 or higher (.xls, .xlsx or .ods formats);
- Presentations – Microsoft Office POWERPOINT version 2003 or higher (.ppt, .pptx or .odp formats);
- Promotional materials (flyers, newsletters) or other non-editable project documents– PDF format;
- For compressed files – ZIP format;
- Bitmap image files – JPEG, PNG or TIFF formats;
- Vector graphics files – EMF or SVG formats;
- Video files - MP4 (H.264 + ACC).

Adhering to these standardised file formats will ensure that documents can be easily shared and read by all Consortium partners, regardless of their operating system or software preferences. Moreover, using these formats will facilitate the preservation of the documents, enabling their retrieval and use in the future.

3.2.4 Document Naming and Coding

To ensure efficient management and easy retrieval of data over time, it is crucial to use a structured file naming convention and maintain consistency in the document reference structure. This approach will create a unique identifier for all CIRAN documents stored on SharePoint. The prescribed naming convention is:

- CIRAN_[DOCUMENT CODE]_[DOCUMENT NAME]_v[VERSION NUMBER]_[CONTRIBUTOR INITIALS]

Examples of this structure are given below for different document types:

- Deliverables shall be named: CIRAN_D.7.1_Plan for Dissemination and Exploitation_v0.3_wef;
- Meeting Minutes shall be named: CIRAN_ Meeting_minutes_ yyyymmdd_v1.0_as.

The version numbering system should be unique and easy to track. The initial draft of the document shall be version 0.1. Subsequent draft versions shall be numbered 0.2, 0.3, and so on. Once the document is finalised and published, it should be assigned version 1.0. If minor changes are made to the published document, the version should be updated to 1.1, 1.2, and so on. For significant changes, the version shall be updated to 2.0. For more detailed information on CIRAN's document naming and coding, please refer to Deliverable 1.1 Project Management Plan.

3.2.5 Data Sharing

To ensure the security and privacy of sensitive data, CIRAN has established rules for data sharing that distinguish two levels of data sharing:

- among Consortium partners;
- with researchers, and the general public.

Data sharing among Consortium partners shall occur through the SharePoint platform or email with a backup in SharePoint. Sensitive data must be anonymised before sharing. When sharing data with researchers outside the Consortium (e.g., data published in Zenodo), special attention must be given to safeguarding the confidentiality of sensitive data. The general public can access deliverables with public dissemination level through the project website and social media, but sensitive deliverables will be kept confidential. The European Commission will have access to the data collected for the deliverables following the procedures outlined in CIRAN's Grant Agreement.

By implementing these rules, CIRAN aims to balance its outreach goals with the need to safeguard privacy and security issues.

3.3 Management of Sensitive Data

To ensure that CIRAN upholds its commitment to protect the confidentiality and privacy of its contributors, it is crucial to exercise the utmost discretion when handling sensitive data (Correia and Falck, 2023). This involves adhering to applicable legal requirements described in Section 2 and implementing appropriate measures to safeguard against unauthorised access, theft, or data loss.

3.3.1 Identification of Sensitive Data

Sensitive data are data that are either private or confidential. The first refers primarily to personal data, and the second refers to data that may also be derived from secondary data shall not be disseminated.

Also, it is worth noting that any response data captured during public consultations are to be considered confidential data and as such must be handled with care.

3.3.2 Keeping Personal Data Private and Anonymisation

To safeguard the privacy and confidentiality of public consultation contributors, it is essential to collect the minimum amount of personal information possible. Such information shall comprise on only those data that are essential to communicate with the participants. For the purpose of research, also relevant topical information, such as membership in a certain stakeholder group may be collected and related to consultation responses. However, such data shall be anonymised as soon as the efficient management of the work permits it. Response data that shall be anonymised as soon as possible in the research process, so that they cannot

be directly attributed to a responder. Non-anonymised information must only be accessible to designated members of WP5 responsible for managing D5.2 and must not be disclosed.

3.3.3 Aggregation of Data

Aggregated data refers to information that combines the responses of several individuals or entities, without revealing the individual responses of each. This can be achieved by grouping data into categories or using summary statistics such as means, medians, and percentages. Any data that could potentially identify an individual or entity must be removed (by the partner that collects and organises the data) or masked (through randomisation, encryption or pseudonymisation)

However, it is important to ensure that the aggregation does not compromise the accuracy or usefulness of the data. CIRAN's primary data must always be reported in publicly available documents in a suitably aggregated form to prevent any contributor from being identified through their response.

3.3.4 Informed Consent

To ensure ethical data collection processes and the protection of individuals' rights, the informed consent of contributors in public deliberations must be obtained prior to interviews or consultation processes. This is a mandatory requirement in accordance with the Ethics Guidelines and a template for informed consent forms can be found in the relevant Deliverable 1.2. Furthermore, it is mandatory to ensure that the data collected from these interviews/consultations are only used for the stated purposes, specified during the interview/consultation process and they must not be used for any other purposes without the explicit consent of the respective contributors. This ensures that confidentiality and the privacy of contributors are respected and protected throughout the project.

3.3.5 Sharing of Data Among the Consortium

If it is necessary to share raw data with entitled Consortium members, it shall not be sent by emails, but through a dedicated private channel on the MS Teams platform. MS Teams data transfers are encrypted to ensure privacy of data in transit. Finally, all personal data will be deleted from the MS Teams channel at the end of the project. A log shall be kept by all data holders of such transfers, recording which data-files when and to whom had been transferred.

3.3.6 Holding Times of Sensitive Data

Sensitive data states must be securely stored and then destroyed no later than 180 days after the completion of the project, which refers to the acceptance of the final report and receipt of payment by the Commission. This protocol serves a dual purpose. Firstly, it enables Consortium partners to access the data if there is any uncertainty regarding the validity of conclusions drawn from it. Secondly, it ensures that sensitive data is not retained for an extended period, thereby minimising the potential risk of unauthorized access or misuse.

3.3.7 Accessibility of Sensitive Data by Persons Concerned

As per the General Data Protection Regulation (GDPR) and the Consortium's Ethics Guidelines (D1.2), individuals have the right to request access to their data that is being held. To ensure compliance, the consent form template includes provisions that prohibit the publication of any data without the contributor's written authorisation. However, if any concerns arise at a later stage, they can be addressed to the contact person mentioned in the consent form, who is responsible for the activity. Alternatively, concerns can be directed to the Project Coordinator via the email address vcorreia@inraw.eu. Upon receiving such concerns, the Project Coordinator shall respond within 10 days and make the necessary changes within a further 10 days. This process ensures that data is handled responsibly and transparently while safeguarding individuals' rights.

3.4 Management of Public Data

CIRAN is tuned to propose inclusive, streamlined policy-making instruments that secure stable and equitable access to the CRMs needed to attain the EU climate goals. Thus, providing access to the underlying data for each project public deliverable will maximise the impact of CIRAN in line with its goals. On the one hand, public data can be re-used by third parties to accelerate their own research, in which way the visibility of CIRAN, as well as that of individual project partners, is increased.

Therefore, disseminating data in a way that makes them Findable, Accessible, Interoperable, and Re-usable (the FAIR principle; Wilkinson *et al.*, 2016) is crucial.

3.4.1 Making Data Findable

CIRAN is committed to transparency and open access in its research activities. To this end, all public deliverables, including datasets, results, and reports, will be published in the Zenodo repository, that assigns DOIs (Digital Object Identifiers) and includes a clear copyright statement. The use of a DOI ensures unique identification of the public dataset and automatised data retrieval via the WWW. Additionally, all public results and datasets will be made available through the project website, social media, and the EU Horizon Results Platform for a minimum of five years after the completion of the project.

CIRAN is dedicated to the principles of open research data and will share all information and data generated by the project and cleared for public access in open formats free of charge with the European Commission for its own use and publication. Datasets not protected by intellectual property rights (IPR) and generated as part of the project's activities will also be made accessible for other projects and initiatives, as part of the Open Research Data initiative.

The data collected or developed by CIRAN include original data sets generated by all Work Packages (WPs), as well as research reports, peer-reviewed journal papers, and synthesis reports. To ensure maximum visibility and impact of the research, top-level scientific articles will be published in Open Access journals.

3.4.2 Making Data Accessible

For maximising the dissemination of CIRAN's results, it is crucial to make data accessible. For doing so, CIRAN will use a Creative Commons license (CC-BY-4.0) and all peer-reviewed publications connected to CIRAN will be Open Access publications (either Green or Gold Open Access). Public datasets will become openly available through CIRAN's website and the Zenodo platform. Relevant meta-data and datasets will be uploaded to this platform, compiling project-related information. This will allow automatic data retrieval ensuring open data access.

3.4.3 Making Data Interoperable

Data interoperability is crucial for facilitating the effective use of data. To achieve this, standardisation is required, as outlined in Section 3.2 of the project documentation. Sections 3.2.3 and 3.2.4 provide detailed specifications for file formats and rules for document coding, respectively.

In addition, it is essential to aggregate data wherever possible, without compromising the value of individual datasets. To achieve this goal, one or more meta-data files will be created for each associated dataset. The meta-data will be identified by the unique ID of the corresponding dataset, using a different suffix or extension. The meta-data files will be linked to the data descriptor and will be directly accessible through Zenodo.

Furthermore, in cases where specific ontologies are used in CIRAN's documents, they will be openly shared to facilitate data interoperability and enable consequent data reuse. This process ensures that data is accessible, usable, and meaningful to users, thereby maximising its potential value.

3.4.4 Making Data Re-Usable

CIRAN aims to make most of its deliverables accessible to the public and relevant practitioners and the envisaged permanent nature of the CIRAN Forum allows for data to be reused effectively.

To ensure the efficient exploitation and dissemination of public deliverables, specific provisions will be defined in the Plan for Dissemination and Exploitation (D7.1) that will be based on the European Commission guidance for science communication for evidence-based policymaking (European Commission Joint Research Centre, 2020). By following this guidance, CIRAN will ensure that all public deliverables are disseminated and exploited correctly to contribute to evidence-based policy-making.

4 Conclusions

CIRAN aims to advance potential pathways for responsible mining in Europe, and achieving this goal necessitates collecting both primary and secondary data. To ensure compliance with the European legislative framework concerning data management, this Data Management Plan (DMP) outlines guidelines for managing data generated or collected in the context of CIRAN.

The first section of the DMP asserts that the CIRAN Consortium fully complies with the General Data Protection Regulation (GDPR) in all its internal conduct documents, such as the Grant Agreement and the Ethics Guidelines (D1.2). Additionally, recognising and respecting Intellectual Property Rights when collecting secondary data is crucial to acknowledge the work of others properly.

The second section of the DMP differentiates between the different types of data to be collected and sets standards for their management. This includes guidelines for data handling, such as document storage, accepted file formats, and establishing a document naming and coding system.

Furthermore, rules for data sharing are defined in this section. Sensitive data shall be kept confidential to protect the privacy and security of the providers. The main ethical and privacy issues related to sensitive data involve ensuring that data remain private and that proper consent is obtained before collecting, processing, sharing or publishing it.

For data and deliverables with a 'public' dissemination level, the primary challenge is to ensure that it is communicated using practices that make them Findable, Accessible, Interoperable, and Reusable (FAIR), while respecting Intellectual Property Rights (IPR).

To guarantee the appropriate dissemination of public deliverables, specific provisions will be outlined in the Plan for Dissemination and Exploitation (D7.1), which will be delivered in the sixth month of CIRAN's implementation.

Effective data management is central to CIRAN's success, and adherence to the guidelines laid out in this document is critical in all phases of the project.

5 Bibliography

Correia, C., Falck., W.E. (2023). *Ethics Guidelines. Deliverable 1.2 of the Critical raw materials extraction in environmentally protected areas (CIRAN) project*. Grant Agreement No. 101091483 of the European Union's Horizon Europe research and innovation programme.

European Commission (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

European Commission Joint Research Centre (2020). *Science for Policy Handbook*. Elsevier Science. ISBN 9780128226902.

The European Union (2012). *Charter of Fundamental Rights of the European Union*. Official Journal of the European Union C83, vol. 53. Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. (2016). *The FAIR Guiding Principles for Scientific Data Management and Stewardship*. *Sci Data* 3, 160018. <https://doi.org/10.1038/sdata.2016.18>. Retrieved from <https://www.nature.com/articles/sdata201618#citeas>.