DMP Evaluation Criteria

focus on project-lifecycle, research discipline and AI-assisted evaluations

Authors

Ahmed E. Mansour, Yasmin Demerdash, Xiaoran Zhou, Antonia Leidel, Marco Reidelbach, Christian Langenbach, Leyla Jael Castro, Juliane Watson, Neelam Vishen, Jürgen Windeck

Version 1.0

April 2026

1. Introduction

Research data management (RDM) involves planning and implementing practices for creating, documenting, storing, sharing, preserving, and reusing data throughout a research project. These practices are formalized and coordinated through a data management plan (DMP), which outlines the roles, responsibilities, standards, and procedures for handling data responsibly and sustainably. DMPs are also expected to adapt dynamically and be updated regularly according to project progress and status as research advances.

Preparing and reviewing DMPs is a core responsibility of RDM professionals, including, data stewards and data officers. Funding agencies increasingly require DMPs as mandatory components of research proposals. This reflects policy-driven expectations of transparency, reproducibility, long-term preservation, and alignment to the FAIR (findable, accessible, interoperable, and reusable) data principles.

Despite their central role, evaluating DMPs remains challenging in practice. Existing DMP templates and guides often provide high-level requirements, yet they lack actionable, domain-specific criteria that enable the systematic evaluation of DMP completeness, consistency, and feasibility. Consequently, DMP reviews are often time-consuming and subjective, depending on the reviewer's expertise. This limits their effectiveness as quality assurance mechanisms and their potential to support FAIR-compliant RDM.

To address this challenge, the *infra-dmp DMP Evaluation Criteria Working Group,* which operates within the *Common Infrastructure Section* of the NFDI, developed a framework for systematically assessing DMPs. Based on the *Science Europe Rubric*, the framework aligns with the lifecycle of research projects and explicitly treats DMPs as *living documents* that evolve over time. The framework distinguishes between different project phases and centers on a guiding question: Is the information provided sufficient for the current phase of the project? This phase-sensitive, iterative approach provides an accurate and constructive assessment, and supports both flexibility and accountability.

The framework supports researchers, RDM professionals, and proposal reviewers by translating funders' requirements into clear, standardized, practical evaluation criteria. This enables a more consistent evaluation across different contexts. Funding bodies such as the Deutsche Forschungsgemeinschaft (DFG) could adopt or adapt the framework to improve the coherence and comparability of DMP review processes.

To further facilitate the consistent and scalable application of these criteria, the DMP-EVA (Data Management Plan Evaluation) tool has been developed. This open-source computational tool is designed to automate the process of checking DMPs against the lifecycle-based criteria presented in this document. The tool provides a technical platform that offers data stewards and reviewers a rapid method for assessing compliance and quality, making the evaluation process more efficient and objective (a short tutorial is shown in Section 5). More details and information on implementation can be found here.

Ultimately, our goal is to empower both data stewards and researchers by providing clear, adaptable, and lifecycle-aware evaluation criteria. In doing so, we aim to promote the development of DMPs that are not only policy-compliant but genuinely useful in guiding the management, sharing, and preservation of research data across disciplines, institutions, and funding contexts.

2. Funding Bodies' Requirements on DMP Update

Evaluating DMPs across the different phases of research projects reflects the growing emphasis of major funding agencies on transparency, accountability, and continuous improvement in handling research data. Many funders explicitly require that DMPs be treated as *living documents,* reviewed and updated as projects evolve. To provide context for the evaluation criteria presented here, we examined the DMP-related requirements of key international and national funders, focusing on their expectations for DMP updates throughout research projects.

These requirements vary significantly across funding bodies, particularly with regard to the timing of initial DMP submission and the frequency and conditions under which updates are required. The following comparative analysis (Table 1) highlights initial submission points, triggers that require updates, and mandated timelines defined by each funder. This analysis clarifies which funders treat the DMP as a living document with regular revision obligations and which primarily require it at the proposal stage with fewer or no formal update checkpoints.

Table 1. Funding Body Update Requirements Overview

Funder	Mandatory submission	Recommended update	Mandatory update
German Research Foundation (DFG), DE	DMP required at proposal submission[1]	Not required	Not required
Horizon Europe, EU	DMP required at proposal submission[2] • Concise DMP at initial submission • Detailed DMP as project deliverable(~ 6 months after project starts)	Project milestones and changes in data management aspects	DMP update is required: • Periodic reporting • Final report
Federal Office for Agriculture and Food (BLE), DE	DMP required at proposal submission[3] • Conceptual DMP at the sketch stage • Detailed DMP at the proposal stage	Changes in data management aspects	DMP update is required: • Interim report • Final report
Volkswagen Foundation, DE	DMP required at proposal submission[4]	Changes in data management aspects	Not required
Carl-Zeiss-Stiftung (CZS), DE	DMP required at proposal submission[5]	Not specified	Not required
Biotechnology and Biological Sciences Research Council (BBSRC), UK	DMP required at proposal submission[6]	Changes in data management aspects	Upon request

Footnote:

[1]The DFG does NOT require a standalone Data Management Plan (DMP) document at proposal submission. Instead, research data management must be addressed explicitly and obligatorily within the proposal. (see the DFG information page on the *handling of research data*)

- For individual research grants, research units, and priority programmes, this is done in Section 2.4 “Handling of research data” of the Project Description. *(see proposal preparation instructions)*
- For Collaborative Research Centers (CRCs / Sonderforschungsbereiche), research data management must be addressed at project level (handling of research data within the individual subprojects). If an Information Infrastructure Project (INF project) is part of the proposal, a CRC-wide concept for data management, access, reuse, and long-term preservation is to be described.*(detailed instructions are provided in the german version of the proposal Template for the Establishment of a Collaborative Research Centre)*

[2] Horizon Europe requires responsible research data management in line with the FAIR principles for all projects generating or reusing data. A full Data DMP is not required at proposal submission; instead, applicants must provide a concise description of planned RDM and open science practices in the proposal. A standalone DMP is mandatory after grant signature and must be submitted by Month 6 as a project deliverable. The DMP is treated as a living document and must be updated throughout the project whenever relevant changes occur (e.g. new data types, access conditions, repositories, or IP considerations), and a final, updated DMP is required with the final report. *(see Horizon Europe programme guide)*

[3] BLE: Applicants must submit a standalone DMP at proposal submission. The DMP is treated as a living document and must be updated and attached to interim reports and submitted in final form with the final report, describing actual data archiving and reuse.

A consortium-wide DMP is required at sketch stage; if a full proposal is requested, each consortium partner must submit an individual DMP with the proposal. *(see Merkblatt zum Forschungsdatenmanagement)*

[4] Volkswagen Foundation requires a DMP for data-generating or data-using projects in disciplines without established data workflows and is typically submitted as a structured Basic Data Management Plan. The Foundation does not define formal mandatory updates, but

recommends treating the DMP as a living document, to be updated when relevant data management aspects change. (see VW open science policy and implementation)

[5] CZS requires a Research Data Concept at the proposal stage for selected programs. The concept is embedded in the proposal, covers core DMP elements, is evaluated during review, and is not required as a standalone or updatable post-award document. No update triggers or timelines are specified. (see for example the call for applications for CZS Nexus 2026)

[6] BBSRC requires applicants to submit a DMP as a separate, mandatory document at the proposal stage for all research grant applications. The DMP is assessed during proposal review and compliance with the proposed data management and sharing plans is monitored during and after the project. Updates to the DMP are expected where necessary to reflect changes in data sharing arrangements, although no fixed update schedule is defined. Applicants may be asked to provide updates or additional information to monitor compliance with the submitted DMP. *(see the BBSRC data sharing policy)*

3. Evaluation Criteria with Focus on Project-Lifecycle

In order to implement our approach of treating DMPs as living documents, this evaluation framework is structured around three key stages of the research project lifecycle: **proposal/early stage**, **mid-project stage**, and **end-project stage**. This structure allows for phase-sensitive evaluations, by explicitly assessing whether the information provided in the DMP is sufficient and appropriate for the project's current stage.

- **The proposal/early stage** focuses on outlining initial data management strategies, ensuring alignment with FAIR principles and funder requirements.
- **The mid-project stage** serves as a crucial checkpoint to review, monitor, and refine practices based on actual project progress, data generation, and emerging challenges.
- **The end-project stage** concentrates on documenting outcomes and implementation, ensuring that data are properly shared, preserved, and documented for long-term accessibility and reuse.

The specific criteria to be evaluated at each stage are detailed in Table 2.

Table 2. General Evaluation Criteria for DMP

Proposal/Early Stage	Mid-Project	End-Project
1 DATA DESCRIPTION AND COLLECTION OR RE-USE OF EXISTING DATA 1a How will new data be collected or produced, and/or how will existing data be re-used?		
For new data collection or production: ☐ Describe the data in terms of scientific context and technical perspective ☐ Specify the methods, tools, instruments, and software to be used for data collection ☐ Justify collecting or producing new data (see Section 1b) ☐ Justify whether proper permissions are obtained for the reuse of personal data from data subjects. For reuse of existing data: ☐ Describe the reused data (type, scope, and relevance) ☐ Explain the purpose of reusing the data (e.g., validation, comparison, integration)	☐ Confirm which data have been produced or reused so far ☐ Update formats and tools used, noting any changes ☐ Include information on data provenance ☐ Update documentation to show growth and technical advances as data is generated	☐ List final data sets, types, and formats collected or reused ☐ Provide justification for deviations from the original plan

Proposal/Early Stage	Mid-Project	End-Project
☐ Mention sources, access conditions, and permissions (e.g., database name, DOI, publication, software, licensing, embargoes, access restrictions)		
1b What data (for example the kind, formats, and volumes) will be collected or produced?		
☐ List expected data types, formats (e.g., open vs. proprietary), and estimated volume (size/number of files) ☐ If proprietary or less-common formats are used, provide justification including any limitations for reuse or access ☐ If the project will not produce new data, clearly state this with an explanation (see Section 1a)	☐ Describe and monitor RDM pipelines and data analysis workflows ☐ Provide technical updates on actual volume, types, and formats produced, noting any technical constraints encountered ☐ Describe data conversion strategies if data will be transformed between formats (e.g., raw to processed formats, proprietary to open)	☐ Archive the final complete set of technical documentation and metadata files ☐ Report on how the final data's technical fidelity can be ensured for reuse
2 DOCUMENTATION AND DATA QUALITY 2a What metadata and documentation (for example the methodology of data collection and way of organising data) will accompany the data? Are method- or discipline specific standards being used? (if so name them)		
☐ Describe the types of metadata to be provided, including both descriptive metadata (e.g., title,	☐ Report which metadata standards or tools are being used ☐ Describe ongoing quality assurance	☐ Provide evidence of complete documentation (e.g., metadata files, ELN snapshots)

Proposal/Early Stage	Mid-Project	End-Project
creator, keywords, project information) and process-related metadata (e.g., experimental or simulation conditions, instrumentation settings, sampling methods, software versions) ☐ List suitable candidates for community metadata standards ☐ Confirm chosen metadata standards align with community best practices and are suitable for the data type and discipline ☐ Mention tools or platforms used for creating and managing metadata (e.g., ELNs, lab management systems, automated metadata capture tools) ☐ Specify the format(s) in which metadata will be stored or shared (e.g., JSON-LD, XML, CSV, RDF)	and quality control (QA/QC) procedures ☐ Explain the rationale for selecting specific metadata standards ☐ If applicable, describe data models or metadata schemas that the project has developed or adopted, including justification for why existing ontologies or vocabularies are not sufficient ☐ Describe how the metadata are stored and shared	☐ Summarize QA outcomes ☐ Describe how metadata will be maintained after the end of the project
2b What data quality control measures will be used?		
☐ Describe the approach to ensuring data quality, including verification	☐ Report on which measures were taken to ensure data quality	☐ Report on the quality control measures taken

Proposal/Early Stage	Mid-Project	End-Project
and validation procedures ☐ Describe measures to track changes and manage versions of data and metadata ☐ Outline quality control steps during data collection and processing (e.g., consistency checks, use of standard procedures, comparison with reference or benchmark data, comparison with control samples) ☐ If applicable, indicate whether the data collection was reviewed by an ethics committee (see Section 4c)		☐ Combine quality control with other criteria, such as ethical, legal, and preservation requirements
3 STORAGE AND BACKUP DURING THE RESEARCH PROCESS 3a How will data and metadata be stored and backed up during the research?		
☐ Provide a storage concept describing where data and metadata will reside during the project (institutional servers, repositories, cloud) ☐ Explain backup or versioning procedures, including methods, frequency, and responsibility	☐ Report where data and metadata are actually stored, and whether this deviates from the initial plan ☐ Document active backup or versioning procedures ☐ Describe the organizational structure for data and associated documentation	☐ List the final storage and backup arrangements for all project data and metadata ☐ Describe how final datasets are transferred to long-term preservation systems that meet recognised security and integrity standards, especially when

Proposal/Early Stage	Mid-Project	End-Project
☐ Note whether institutional IT or RDM services provide storage or backup support ☐ If personal data is involved, include a clear statement that all storage locations comply with institutional security standards and GDPR requirements. Add that researchers should specify whether a Data Processing Agreement is needed for any external storage service.	☐ Confirm that backups, versioning, and storage security have been tested and that any deviations from institutional policy are documented and approved.	involving personal data.
3b Who needs access to the data? Are there legal aspects that have to be considered (to limit access)?		
☐ Clarify user roles (e.g., PhD students, collaborators, data stewards) and access levels. ☐ Identify any personal or sensitive data (e.g., data sensitivity, confidentiality, IP), and justify why certain users require access. ☐ Outline how access will be granted and documented (e.g., user accounts, project folder structure, institutional authentication)	☐ Update the access rights (authentication and authorization) of individuals or teams currently having access, reflecting staff or collaboration changes, including the removal of users who no longer require access. ☐ Specify intended levels of access (e.g., read-only, edit, administrative) for different users or groups ☐ Note how access monitoring or	☐ Specify how access will be discontinued and how external access requests will be handled after completion.

Proposal/Early Stage	Mid-Project	End-Project
	audit logs are maintained, either by the project or institutional IT	
3c How will data security and protection of personal or sensitive data be taken care of during the research?		
☐ Identify whether sensitive, personal (Data protection basics), or confidential data will be handled and what makes them sensitive (e.g., personal identifiers, proprietary results, trade secrets; see Section 4a) ☐ Describe the planned security approach for data storage and transfer (e.g., encrypted drives, secured servers, controlled network access, physical restrictions) ☐ Explain how access to personal or sensitive data will be restricted (e.g., password protection, role-based permissions) ☐ Mention relevant institutional or national data-protection policies (e.g., GDPR compliance statement or link)	☐ Confirm which personal and sensitive data have actually been collected or processed and where they are processed and stored ☐ Describe how security measures have been implemented (e.g., encryption enabled, access logs maintained) ☐ Show that data-protection responsibilities are clearly assigned within the project or to institutional services ☐ Report any security incidents or near misses, along with the steps taken to address them. Document the incident and follow project/institutional procedures for an incident response plan. ☐ Indicate how data transfers or collaborations are secured (e.g.,	☐ Confirm that all personal and sensitive data are securely stored, anonymized, or deleted according to institutional and legal requirements ☐ Document the final security configuration and provide references to institutional policies or repository standards followed ☐ Summarize how security and privacy obligations were fulfilled, including GDPR or contractual requirements ☐ Describe how long-term archived or retained data will remain protected (e.g., repository with certified security standards)

Proposal/Early Stage	Mid-Project	End-Project
☐ Specify which support services or responsible offices (e.g., data-protection officer, IT security) will assist the project ☐ Outline a basic incident-response or recovery plan in case of data loss or breach	VPN, encrypted exchange platforms)	
4 LEGAL AND ETHICAL REQUIREMENTS, CODES OF CONDUCT 4a If personal data are processed, how will compliance with legislation on personal data and security be ensured? ⚠ Please note that the listed legal requirements only need to be completed when they apply to the project. If they do not apply, a statement is sufficient.		
☐ Describe the legal basis for processing under GDPR Article 6, and if applicable, the exemption under Article 9(2)(j) for scientific research or use of explicit consent and how data subjects are informed. ☐ If applicable, especially in complex scenarios when the consent cannot be taken back, or the public interest is claimed, document the justification of the legal basis.	☐ Confirm that records of processing activities relating to personal data have been created or updated according to institutional or legal requirements, if necessary ☐ Confirm that the legal basis for processing has been formally documented and, if applicable, that informed consent has been obtained or justified and subjects are informed about processing and reuse if planned	☐ Confirm that all data protection measures were implemented and monitored throughout the project lifecycle ☐ Describe how personal data has been securely deleted, anonymized, or retained in line with the approved retention schedule ☐ State whether any personal data will be reused and on what legal basis ☐ Confirm that any published outputs

Proposal/Early Stage	Mid-Project	End-Project
☐ Confirm the expected roles of data controller(s) and processor(s), including institutional and external parties ☐ State whether a (Data Protection Impact Assessment (DPIA) is likely to be required, and when it will be conducted ☐ Discuss if there are any possible data transfers outside the EU ☐ Describe initial plans for pseudonymization and/or anonymization ☐ Summarize the intended technical safeguards (e.g., secure storage, encryption, access control; see Section 3c) ☐ Reference relevant institutional support (e.g., contact with Data Protection Officer, planned ethics submission) ☐ Mention any planned data processing, use, or transfer	☐ Confirm completion of a DPIA, if required ☐ Describe the technical and organizational measures actually implemented, or reference the institutional Technical and Organisation measures(TOMs) that apply to your project ☐ Identify the data storage locations and systems in use, confirming institutional approval and security standards (see Section 3c) ☐ If data is to be transferred outside the EU, reference the Transfer Impact Assessment (TIA) and revisit the idea and make changes depending on the result of the TIA. ☐ List any signed agreements (e.g., DPA with core facilities, DUAs with collaborators, SCCs for international transfers). These details and any copies could also be included in the ROPA Art. 30 GDPR - Records of	or deposited datasets have been anonymized or shared under appropriate controlled access conditions ☐ Describe how compliance documentation, such as the ROPA, DPIA, consent forms, and agreements, will be archived or made available for audit ☐ Document and show how the project ensures that personal data is absent from outputs made public, and if there is an exception, provide a documented justification

Proposal/Early Stage	Mid-Project	End-Project
agreements (e.g., DPA, DUAA, SCCs)	processing activities GDPR.eu, https://gdpr.eu/article-30-records-of-processing-activities/ (last visited Dec 5, 2025) of that processing activity if a ROPA was created. ☐ Describe how ethics approval, risk assessments, or external audits are being managed ☐ Update any changes to the scope of personal data processing or data sharing ☐ Create a ROPA (Record of Processing Activities) if needed. That gives you an overview of everything about that processing activity, including what data, who the data subjects are, the purpose of data processing, where it is stored, like a proper data mapping if properly filled. Talk to your legal team for support if need be	
4b How will other legal issues, such as intellectual property rights and ownership, be managed? What legislation is applicable?		
☐ Identify elements that may involve	☐ Confirm whether any new outputs	☐ Confirm the final ownership status

Proposal/Early Stage	Mid-Project	End-Project
legal issues, or state that there are no legal restrictions ☐ Identify the anticipated data outputs (e.g., datasets, software, protocols) that may be subject to IPR ☐ Clarify whether third-party data, software, or materials subject to licensing conditions will be used and how compliance with those licences will be managed ☐ Describe who will own the data and results ☐ Mention whether collaboration agreements, joint IP agreements, or employment contracts define ownership and access rights ☐ Summarize relevant legal frameworks (e.g., national copyright law, institutional IP policies, Nagoya Protocol) ☐ State whether IP and authorship will be handled by a technology transfer office (TTO) or legal department	require licensing decisions and whether licence compatibility has been reviewed for datasets, software, or documentation. ☐ Confirm that any relevant IP or data ownership clauses or other legal issues have been formalized in signed agreements (e.g., collaboration agreements, DUAs) ☐ Describe how access rights to data are managed internally and with partners ☐ Confirm who holds the right to publish results and reuse data after project completion ☐ Identify who is responsible for maintaining records of IP decisions or agreements	and other legal issues of data and outputs ☐ Describe how access and reuse of data will be managed post-project (e.g., open access, embargoed, restricted) ☐ Note that any restrictions to data sharing should be explained in Section 5a ☐ List any registered IP (e.g., software licenses, patents) resulting from the project ☐ Summarize how legal or contractual obligations were fulfilled regarding ownership and reuse ☐ Confirm that collaborators and institutions are aware of their ongoing rights or restrictions related to the data

Proposal/Early Stage	Mid-Project	End-Project
☐ Check if ethical issues are a major concern in the project (e.g., health or animal research) ☐ Describe the need for ethics approval from an ethical committee, and whether it has been applied for or is planned ☐ Describe any ethical considerations related to participant recruitment, sampling strategies or participant burden. Do cultural, social or community-specific factors require additional ethical attention? ☐ Explain how participants will be informed about the study purpose, procedures and any potential risks or discomforts. ☐ Indicate whether the project involves vulnerable groups and how their participation is ethically safeguarded. ☐ List the responsible person and check procedures if needed	☐ Confirm that ethics approval has been obtained, and list the approving body ☐ Summarize any changes to ethical considerations (e.g., new data sources, new populations) ☐ Note whether changes in recruitment, sampling, or study populations introduced new ethical considerations	☐ Confirm ethical issues have been fulfilled and documented ☐ Confirm that any published data or materials comply with ethics approvals and participant agreements ☐ Describe how end-of-study obligations were handled, such as debriefing or communicating results to participants where appropriate

Proposal/Early Stage	Mid-Project	End-Project
☐ List the existing relevant codes of conduct or standards, if needed		
5 DATA SHARING AND LONG-TERM PRESERVATION 5a How and when will data be shared? Are there possible restrictions to data sharing or embargo reasons?		
☐ Provide a clear plan for data sharing, describing what data will be shared, where, and when (e.g., via a trusted repository upon publication or after a defined embargo) ☐ If data cannot be shared, provide a plan for sharing the metadata as an alternative ☐ If data cannot be shared, explain how the "good scientific practices" of storage for 10 years will be handled	☐ Identify actual repositories used or selected ☐ Note any updates to sharing timelines or formats ☐ Ensure internal sharing of metadata and data regularly	☐ Specify the license for reuse (e.g., CC BY, CC0) ☐ If data cannot be shared (e.g., for legal, ethical, or commercial reasons), explain valid restrictions and access conditions (see Section 4a) ☐ For sensitive data requiring restricted access, clearly state access conditions and procedures ☐ Specify the timing of data availability, including any embargo periods and justifications
5b How will data for preservation be selected, and where will data be preserved long-term in a suitable archive? (for example a data repository or archive)		
☐ Describe the criteria for selecting which data and metadata will be preserved long-term (e.g., final validated data, high-impact	☐ Identify actual datasets being planned to be stored in the repositories; note any updates ☐ Report any updates on selection	☐ Confirm datasets have been deposited in the repository or archive with appropriate metadata, licenses, and PIDs; explain

Proposal/Early Stage	Mid-Project	End-Project
datasets, representative samples) ☐ Name potential repositories or archives for long-term preservation ☐ If no repository is used, explain the storage plan in detail ☐ State the planned retention period (e.g., 10+ years), ensuring it aligns with funder or community expectations	criteria or retention period ☐ Confirm chosen archiving solution / repository for long-term preservation	deviations
5c What methods or software tools are needed to access and use data?		
☐ List the planned file formats ☐ Prefer open, non-proprietary formats; if proprietary formats are used, acknowledge and justify this ☐ List the planned tools or software to access, visualize, or analyze the data	☐ Update tools or software required to access, visualize, or analyze the data. Prioritize open-source tools or recommend them where possible ☐ If proprietary tools are required, provide alternatives or rationale ☐ Update file formats	☐ Confirm file formats used for preservation are listed ☐ Recommendation: provide both proprietary and open format, if possible, for smaller datasets ☐ Confirm tools or software required to access, visualize, or analyze the data are named ☐ Describe access mechanisms clearly (e.g., via a GUI, API, or direct download) ☐ If applicable, include or link source code or workflows needed to

Proposal/Early Stage	Mid-Project	End-Project
		interpret the data (e.g., analysis scripts, custom parsers, or notebooks), ideally under an open license
5d How will the application of a unique and persistent identifier (such as a Digital Object Identifier (DOI)) to each data set be ensured?		
☐ Plan using persistent identifiers ☐ If no persistent identifiers are planned, provide justification (e.g., internal use, access limitations, early-stage data)		☐ Provide a list of published datasets and their PIDs ☐ Ensure that identifiers are linked with metadata to support findability, citation, and reuse
6 DATA MANAGEMENT RESPONSIBILITIES AND RESOURCES 6a Who (for example role, position, and institution) will be responsible for data management (i.e. the data steward)?		
☐ List the roles and responsibilities of all relevant project stakeholders in relation to data management (e.g., principal investigator, researchers, data steward, IT staff) ☐ Assign responsibilities for key data-related tasks: data acquisition and storage, metadata creation and documentation, backup and recovery procedures, repository submission and long-term	☐ Confirm actual roles and effort committed; monitor whether responsibilities are fulfilled in practice ☐ Identify any bottlenecks or overlaps in data-related tasks and adjust accordingly ☐ Ensure replacement or onboarding procedures for team members ☐ Update RDM documentation to reflect current team structure	☐ Finalize and document the complete list of contributors and institutional support ☐ Reflect on the adequacy of assigned resources and responsibilities

Proposal/Early Stage	Mid-Project	End-Project
preservation, compliance with institutional/funder/legal data policies ☐ Address who will be responsible for maintaining access and managing data after the end of the project (e.g., institutional support, long-term repository)		
6b What resources (for example financial and time) will be dedicated to data management and ensuring that data will be FAIR (Findable, Accessible, Interoperable, Re-usable)?		
☐ Provide preliminary estimates of human, financial, and technical resources for data management (e.g., time commitments, infrastructure needs, repository fees, staff time in person-days or FTE) ☐ Identify planned external or institutional support (e.g., consortia services, RDM training) ☐ Mention plans for external support (e.g., from national infrastructures, consortia, or service providers), if	☐ Review actual resource allocation and expenditures ☐ Monitor workload against estimates and adjust where necessary ☐ Assess sufficiency of storage, software, and training provisions ☐ Document any additional support acquired	☐ Summarize total resources spent and their impact on data management effectiveness ☐ Evaluate cost-efficiency and adequacy of FAIR implementation ☐ Provide a final report on institutional and external support contributions

Proposal/Early Stage	Mid-Project	End-Project
applicable ☐ Acknowledge support from institutional infrastructure or services (e.g., data storage, backup systems, RDM training)		

4. Discipline-Specific Guidance

While the general evaluation framework presented in Section 3 provides a consistent, phase-sensitive structure for all DMPs, effective data management requires the integration of domain-specific standards. Different research areas, such as physics, plant biology, or materials science have unique data types, metadata standards, and workflows. These nuances necessitate a tailored approach to evaluation.

To address this, the general criteria are complemented by discipline-specific guidance. This section introduces specialized evaluation components that allow data stewards and reviewers to assess compliance not only with funder mandates and FAIR principles but also with the specific, accepted best practices within a given scientific field. By incorporating this layer of specificity, the framework ensures that DMPs are not only compliant on a procedural level but are also genuinely useful for managing data in a researcher's particular context.

Material Science: FAIRmat
Plant Science: DataPLANT (FAIRagro)
Additional disciplines: Community contributions are welcome

5. AI Assisted Evaluation by using DMP-EVA Tool

The consistent and scalable application of this lifecycle-aware evaluation framework is technically supported by the open-source DMP-EVA (Data Management Plan Evaluation) tool. This tool automates the process of checking DMPs against the criteria established in this document, offering a rapid and objective quality assessment.

For users, the DMP-EVA tool is designed for ease of access and application. Detailed steps for setting up and running the evaluation are provided in Fig. 1.

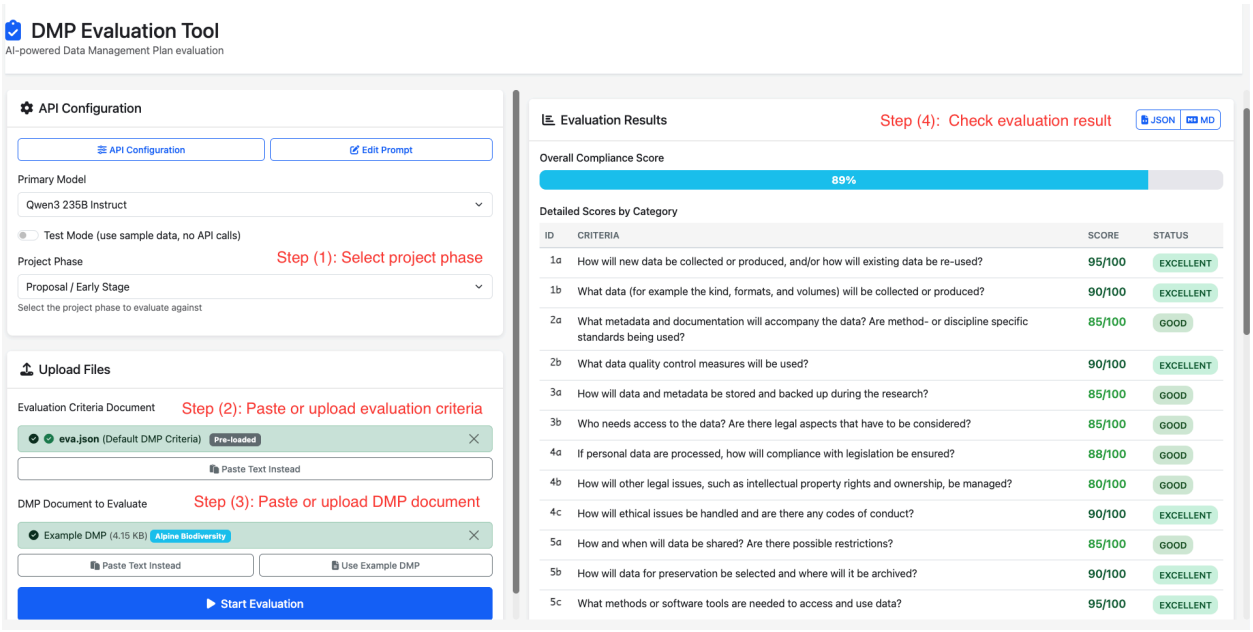

Figure 1. The DMP-EVA tool supports DMP evaluation in four steps.
Step 1: Select the appropriate project phase from three options: early-, mid-, or end-project phase.
Step 2: Paste or upload the evaluation criteria for DMP assessment. The criteria listed in Table 2 are preloaded as eva.json. Users may also upload or define their own evaluation criteria.
Step 3: Paste or upload the DMP document to be evaluated. Plain text (.txt) or Markdown (.md) formats are recommended, as they can be processed directly without pre-processing. Microsoft Word documents are partially supported and are automatically converted to Markdown format. Users are required to review and validate the converted document before proceeding with the evaluation.
Step 4: Review the evaluation results at both the overview level and the sentence level.

6. Contributing and Feedback

This is a living, community-driven resource. We welcome:

- Discipline-specific guidance contributions
- Adaptations for specific funder requirements
- Feedback on criteria applicability and clarity

You are invited to our github organization https://github.com/orgs/dmp-evaluation for contributions and discussions.

7. Acknowledgments

We appreciate the feedback from the infra-dmp Working group and participants during our workshops.

8. List of abbreviations

Abbreviation	Full Name / Description	Category
API	Application Programming Interface	Technical
ARC	Annotated Research Context (DataPLANT Platform)	Research Management
BBSRC	Biotechnology and Biological Sciences Research Council (UK)	Funding Body
BLE	Bundesanstalt für Landwirtschaft und Ernährung (Federal Office for Agriculture and Food)	Funding Body
CC BY 4.0	Creative Commons Attribution 4.0 (License)	Data Standards
CC0	Creative Commons Zero (Public Domain Dedication)	Data Standards
CRC	Collaborative Research Center (Sonderforschungsbereich)	Research Management
CSV/TSV/PSV	Comma-Separated, Tab-Separated, Pipe-Separated Values (File formats)	Data Formats
CZS	Carl-Zeiss-Stiftung	Funding Body
DFG	Deutsche Forschungsgemeinschaft (German Research Foundation)	Funding Body
DMP	Data Management Plan	Research Management
DOCX	DOCument eXtended (Microsoft Word file)	Data Formats

DOI	Digital Object Identifier	Data Standards
DPA	Data Processing Agreement	Legal/Ethical
DPBO	DataPLANT Biology Ontology	Technical
DPIA	Data Protection Impact Assessment	Legal/Ethical
DUA	Data Use Agreement	Legal/Ethical
ELN	Electronic Lab Notebook	Technical
EU	European Union	Geographic
FAIR	Findable, Accessible, Interoperable, and Reusable (Data Principles)	Research Management
FTE	Full-Time Equivalent (staff time measure)	Research Management
GDPR	General Data Protection Regulation	Legal/Ethical
GUI	Graphical User Interface	Technical
INF	Information Infrastructure (Project)	Research Management
infra-dmp	infra-dmp (Working Group Identifier)	Other
IP	Intellectual Property	Legal/Ethical
IPR	Intellectual Property Rights	Legal/Ethical
JSON-LD	JavaScript Object Notation for Linked Data	Data Formats
LLM	Large Language Model	Technical
NFDI	Nationale Forschungsdateninfrastruktur (German National Research Data Infrastructure)	Research Management

OBO	Open Biomedical Ontologies (Foundry)	Technical
PDF	Portable Document Format	Data Formats
PID	Persistent Identifier	Data Standards
QA/QC	Quality Assurance/Quality Control	Technical
QC	Quality Control	Technical
RDF	Resource Description Framework	Data Formats
RDM	Research Data Management	Research Management
ROPA	Record of Processing Activities	Legal/Ethical
SCCs	Standard Contractual Clauses (for international data transfers)	Legal/Ethical
TIA	Transfer Impact Assessment	Legal/Ethical
TOMs	Technical and Organizational Measures	Legal/Ethical
TTO	Technology Transfer Office	Research Management
VPN	Virtual Private Network	Technical
XML	eXtensible Markup Language	Data Formats

9. Generative AI usage declaration

The following generative AI tools were used in the preparation of this document: Gemini, ChatGPT, Claude, and Qwen. Their use was limited to refining the text, specifically for:

- Formatting the text.
- Checking grammar and spelling.
- Improving the overall structure.

Following the generation of AI-assisted content, all output was rigorously checked and modified by the authors. The authors of this document take full and final responsibility for the content, accuracy, and integrity of the resulting text.