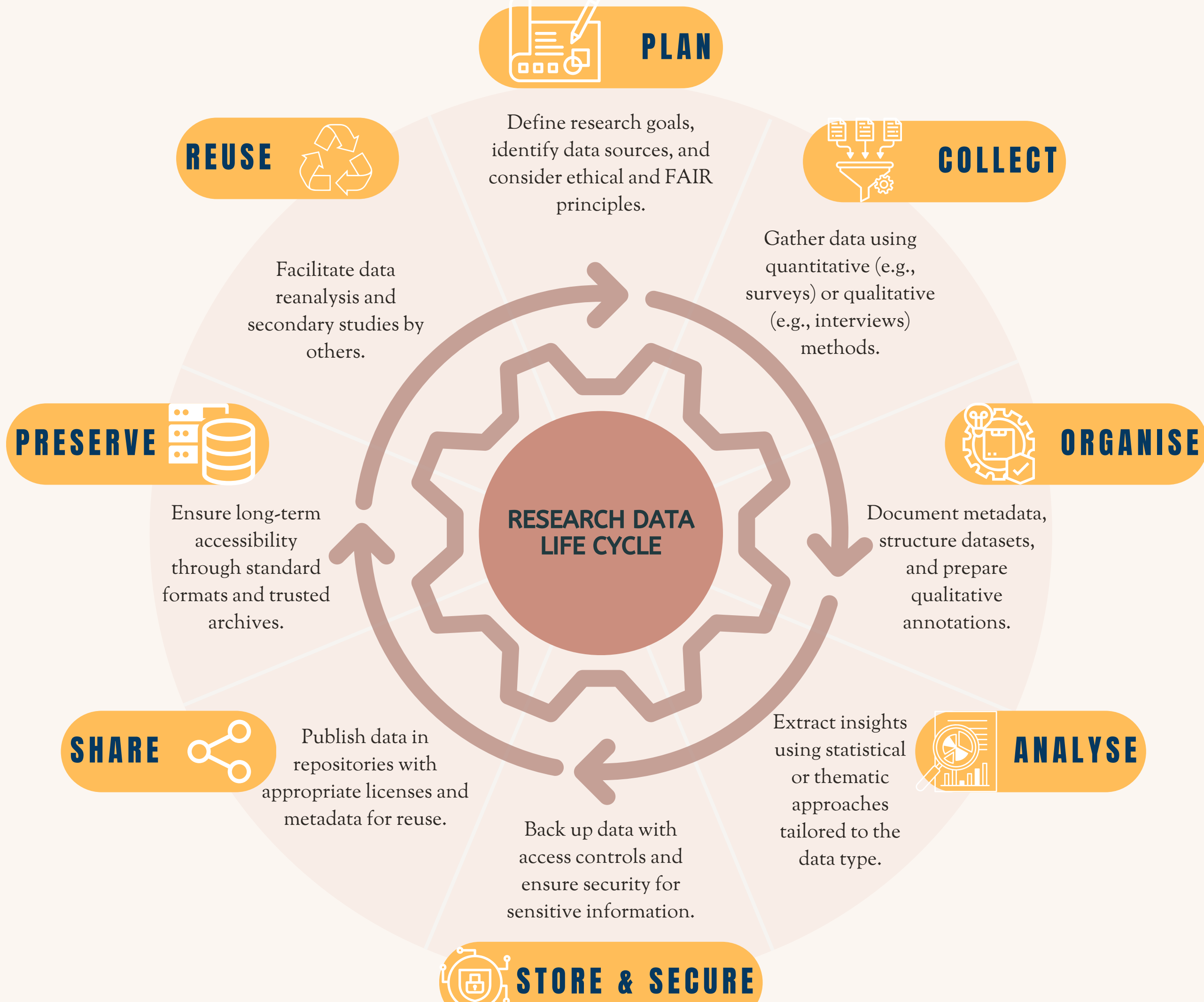
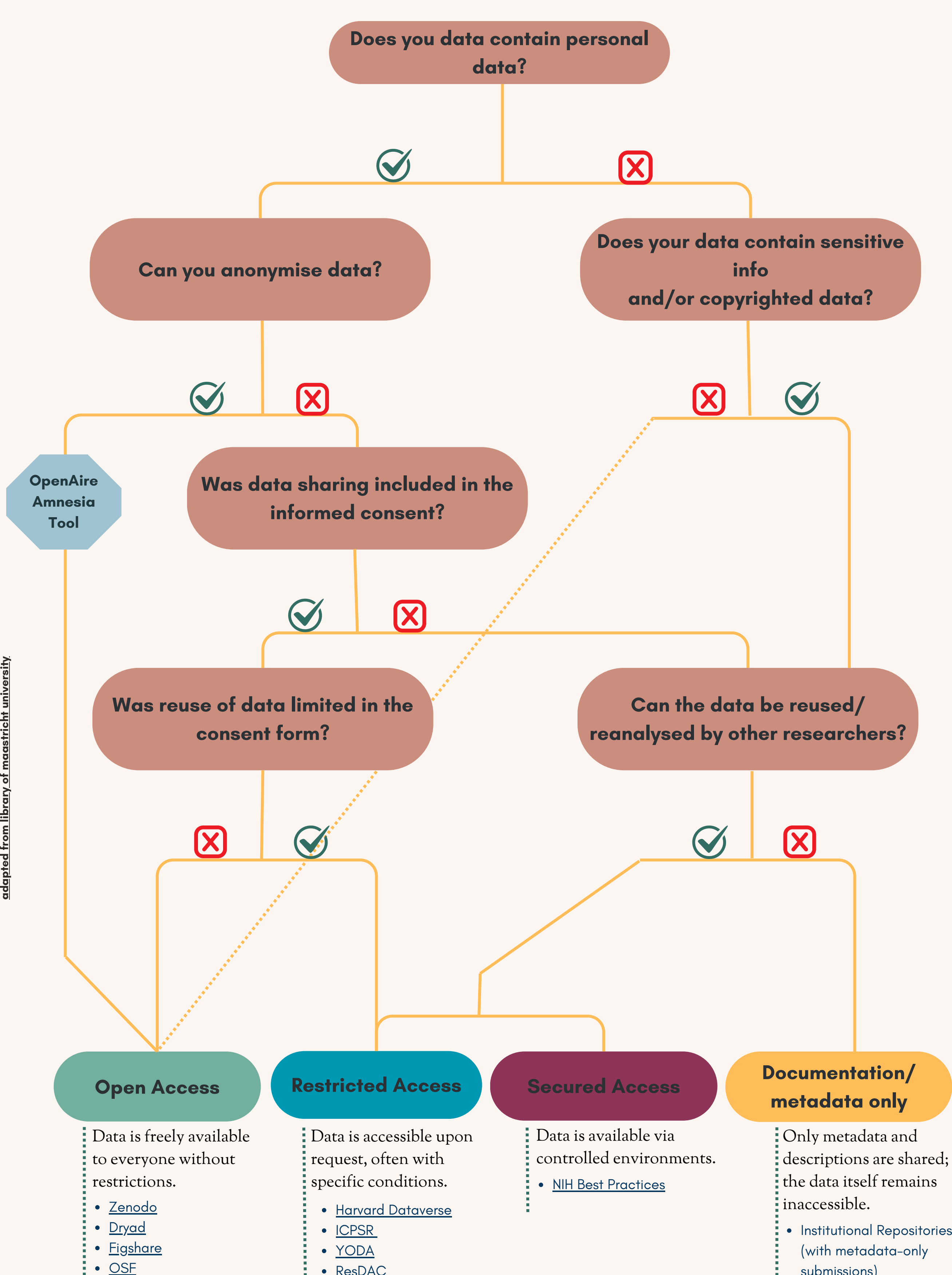


A Data Management Plan (DMP) serves as the blueprint for implementing the FAIR principles, outlining how data will be collected, organised, stored, and shared to ensure it remains Findable, Accessible, Interoperable, and Reusable. In the context of Data Management, "data" is understood in a broad sense, encompassing all research outputs, whether quantitative or qualitative, including research materials, protocols, code, models, interviews, transcripts, case studies, videos, and more. Data management ensures the consistency, accessibility, and reusability of data across the entire data life cycle, from collection and documentation to storage, sharing, and long-term preservation.



When determining how to share data and the level of openness, it is essential to consider the type of data, its sensitivity, any proprietary restrictions, and ethical concerns, ensuring that the sharing process aligns with legal, institutional, and community standards while protecting privacy and confidentiality. The flowchart below helps determine the appropriate level of data openness, accounting for the nature of the data—whether qualitative, quantitative, or mixed—and the specific context in which it is collected.



After identifying the appropriate access level for data, the next step involves developing a comprehensive Data Management Plan (DMP). A strong DMP incorporates six core elements that address all stages of data handling and sharing. These components form the foundation of effective data management practices, facilitating responsible sharing and reusability. More precisely, a strong DMP answers the following questions:



1. Data description and collection or re-use of existing data

- How will new data be collected or produced and/or how will existing data be re-used?
- What data (for example the kinds, formats, and volumes) will be collected or produced?



2. Documentation and data quality

- What metadata and documentation (for example the methodology of data collection and way of organising data) will accompany data?
- What data quality control measures will be used?



3. Storage and backup during the research process

- How will data and metadata be stored and backed up during the research process?
- How will data security and protection of sensitive data be taken care of during the research?



4. Legal and ethical requirements, codes of conduct

- If personal data are processed, how will compliance with legislation on personal data and on data security be ensured?
- How will other legal issues, such as intellectual property rights and ownership, be managed? What legislation is applicable?
- How will possible ethical issues be taken into account, and codes of conduct followed?



5. Data sharing and long-term preservation

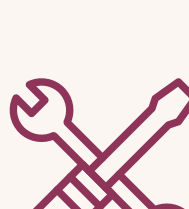
- How and when will data be shared? Are there possible restrictions to data sharing or embargo reasons?
- How will data for preservation be selected, and where will data be preserved long-term (for example a data repository or archive)?
- What methods or software tools will be needed to access and use the data?
- How will the application of a unique and persistent identifier (such as a Digital Object Identifier (DOI)) to each data set be ensured?



6. Data management responsibilities and resources

- Who (for example role, position, and institution) will be responsible for data management (i.e. the data steward)?
- 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)?

source: Science Europe



Tools to Help Create and Manage a Data Management Plan (DMP)

DMPonline & DMPTool

Templates and guidance for creating DMPs tailored to specific funder requirements.

Argos (OpenAIRE)

Templates to create machine-actionable DMPs that align with the FAIR principles for data sharing.

RSpace

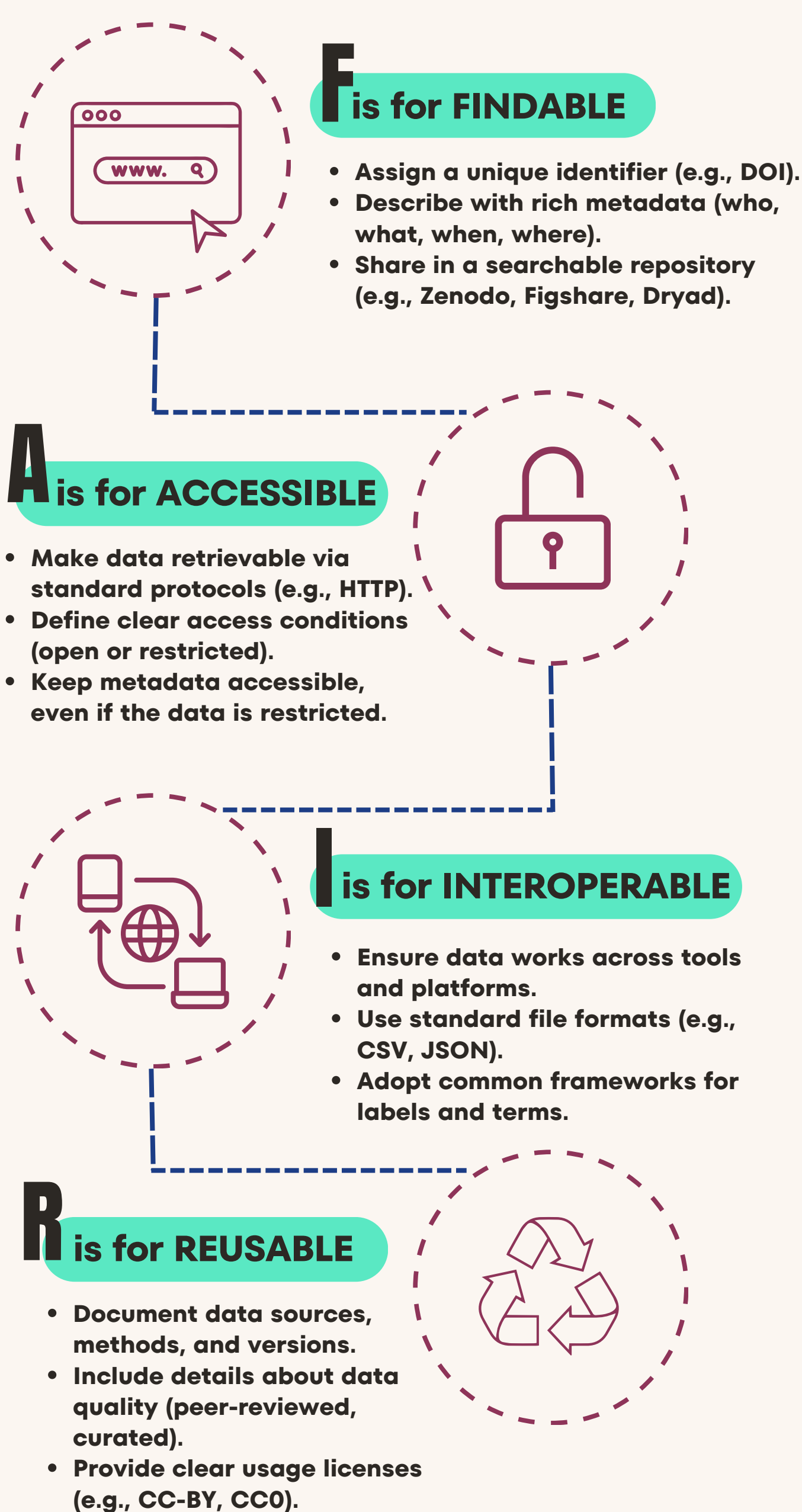
A digital lab notebook that incorporates DMP tools, allowing you to manage data and link it directly to your plan.



Create your own DMP

FAIR & Open Data

The FAIR principles (Findable, Accessible, Interoperable, Reusable) provide a framework for ensuring that research data is structured and shared in ways that maximise its accessibility and utility, not just during your project but for future use by others. These principles can be extended beyond data to include software code, algorithms and models, tools and instruments, educational materials, and other outputs. By adhering to these principles, you set the stage for making your data more impactful, collaborative, and sustainable across disciplines.



FAIR Data vs. Open Data: What's the Difference?

While FAIR Data and Open Data are complementary concepts, they are not the same:

- **FAIR Data:**

The FAIR principles focus on making data Findable, Accessible, Interoperable, and Reusable, regardless of whether the data is openly available. FAIR data doesn't necessarily have to be open—it can include data that is restricted or controlled due to ethical, legal, or proprietary concerns, as long as it is well-documented, structured, and reusable under specified conditions.

- **Open Data:**

Open data refers to data that is freely accessible to anyone without restrictions, provided ethical and legal considerations (e.g., privacy, confidentiality) are respected. Open data aligns with FAIR principles when properly documented and formatted for reuse.

Data can be FAIR without being open, but making open data FAIR enhances its usability and value for the research community.


Alternatives to Open Data


For cases where open data is not feasible, researchers can adopt controlled sharing mechanisms that still adhere to FAIR principles:


- **Anonymisation:** Remove or mask personal or sensitive identifiers in datasets to protect privacy while enabling broader sharing.
- **Data Sharing Agreements:** Restrict access to authorised users while ensuring proper documentation and reuse conditions.
- **Embargoed Data:** Temporarily restrict access until certain conditions are met (e.g., after publication or a set timeframe).
- **Restricted Access Repositories:** Host data in repositories where access is granted based on applications or user credentials.


As open as possible, as closed as necessary.
Aim to share your data responsibly while ensuring compliance with regulations and protecting sensitive information.



 [Learn more about Data Sharing](#)

 [Learn more about Open Code/Software](#)

 [Learn more about Open Qualitative Data](#)

 [Learn more about Licensing your Data](#)