Plan Overview

A Data Management Plan created using DeiC DMP

Title: Sleep Difficulties After Loss: Exploring the Beneficial Effect of Brief Behavioral Therapy for Insomnia in a Sample of Bereaved Individuals

Creator: Alexander Castro-Pavlik

Principal Investigator: Alexander Castro-Pavlik

Data Manager: Alexander Castro-Pavlik

Project Administrator: Alexander Castro-Pavlik

Affiliation: Aarhus University

Template: DCC Template

ORCID iD: 0009-0005-3322-4291

Project abstract:

The study is a randomized controlled trial comparing the effect of a brief behavioral therapy for insomnia (BBTI) on insomnia with an active control group (sleep hygiene). Participants will be 58 bereaved individuals who experience insomnia. After baseline assessment, participants will be randomized to either BBTI or sleep hygiene (active control). Both groups will undergo post-treatment assessments as well as 3- and 6-months follow-up assessments. The primary outcomes will be insomnia assessed with the Insomnia Severity Index (ISI) and improvements in sleep quality using the Pittsburgh Sleep Quality Index (PSQI) and sleep parameters using the consensus sleep diary. The secondary outcome will be complicated grief reactions (CGR) using the Aarhus Prolonged Grief Disorder scale (A-PGDs, prolonged grief). the Center of Epidemiological Studies Depression Scale (CESD-10, depression), the General Anxiety Disorder-7 questionnaire (GAD-7; anxiety), and the short-form PTSD Checklist for DSM-5 (PCL-5; PTSD).

The study has the following aims and hypotheses:

PRIMARY AIM: To investigate whether BBTI improves sleep in bereaved patients screened for insomnia when compared to an active control group.

PRIMARY HYPOTHESIS: Compared with the active control group, participants receiving BBTI will show statistically significant reductions in insomnia using the ISI, as well as improvements in sleep quality using the PSQI and sleep parameters using the consensus sleep diary.

SECONDARY AIM: To explore whether BBTI improves CGR in bereaved patients screened for insomnia when compared to an active control group.

SECONDARY HYPOTHESIS: Compared with the active control group, participants receiving BBTI will show statistically significant reductions in CGR using the A-PGDs, the CESD-10, the GAD-7, and the PCL-5.

ID: 7862

Start date: 30-12-2025

End date: 31-05-2027

Last modified: 03-12-2025

Copyright information:

Sleep Difficulties After Loss: Exploring the Beneficial Effect of Brief Behavioral Therapy for Insomnia in a Sample of Bereaved Individuals

Data Collection

What data will you collect or create?

Type, format and volume of data
The project will generate **quantitative survey data**, **sleep diary entries**, and **study administrative data** related to participant progress through the intervention. The primary data types include self-reported measures collected at multiple time points (T1–T5), session-related data from treatment delivery, and sleep diary information collected both digitally and in some cases on paper before digitalisation. These data consist mainly of structured numerical and categorical variables, as well as limited free-text comments from participants.

All digitally collected data are stored in **REDCap** (Aarhus University-hosted instance) and exported in standard, non-proprietary formats such as **CSV**, **TXT**, or **JSON**, depending on analytical needs. These formats ensure interoperability, long-term accessibility, and facilitate later reuse or archiving. Any paper-based materials (e.g., handwritten sleep diaries or therapeutic worksheets) are scanned and stored as **PDF** files before being transferred to the secure AU infrastructure (**SIF**) in accordance with AU's data-protection procedures.

The total data volume is expected to be **modest** (well below a few gigabytes) and easily manageable within AU's secure storage capacity. Storage requirements are therefore minimal, and AU's infrastructure sufficiently supports versioning, backups, and controlled access.

Suitability of chosen formats and software for sharing and long-term access
The use of **CSV** and **PDF** ensures long-term readability and avoids dependence on proprietary software. REDCap supports structured data collection, audit trails, and export to widely used statistical packages (e.g., SPSS, R, and Stata). These choices ensure that the data can be archived and shared in compliance with institutional and legal requirements, once appropriately pseudonymised or anonymised.

Reuse of existing data
No pre-existing datasets or third-party data sources will be reused in this project. All data are generated specifically for the purposes of the study and originate directly from participant questionnaires, sleep diaries, and treatment-related activities.

How will the data be collected or created?

Data will be collected using established, standardised research instruments (e.g., validated psychological questionnaires and structured sleep diaries). All electronic data will be collected through **REDCap**, which enforces predefined variable structures, branching logic, validation rules, and controlled vocabularies. The methodology for data collection follows consistent protocols across participants and time points (T1–T5), ensuring comparability and standardisation. Paper-based sleep diaries or treatment materials are digitised in a uniform manner using PDF format and uploaded to AU's secure infrastructure (**SIF**), ensuring consistent metadata and file structure.

Folder and file structure
Data will be stored in a hierarchical folder structure on SIF designed to support security and clarity:

- 00_Administration
- 01_Raw_Data (exports from REDCap; scanned paper materials)
- 02_Clean_Data (pseudonymised, quality-checked datasets)
- 03_Code (analysis scripts)
- 04_Documentation (data dictionaries, codebooks, decisions logs)
- 05_Results (derived outputs, figures, tables)

Files will follow consistent naming conventions such as:
Study3_Dataset_RAW_YYYYMMDD.csv
Study3_SleepDiary_ParticipantID_Date.pdf
Study3_TxSessionLog_ParticipantID_v01.csv

This structure supports transparency, ease of navigation, and long-term preservation.

Versioning
Version control will be applied throughout the project. Raw data exports from REDCap are stored as immutable files with timestamps. Data cleaning and transformation scripts (e.g., in R, Python, or SPSS) are version-controlled, and revised datasets include incremental version numbers (e.g., v01, v02). This ensures full reproducibility and traceability from raw to final analytical datasets. REDCap's built-in audit trails also track any changes to forms, metadata, and user interactions.

Quality assurance processes
Multiple quality assurance measures will be used:

- **Standardised data capture:** REDCap enforces validation (e.g., numeric ranges, mandatory fields) to minimise data-entry errors.
- **Controlled vocabularies:** Categorical variables are predefined to prevent inconsistent entries.
- **Double-checking paper-to-digital transfers:** Scanned materials are reviewed before upload, and a subset is double-checked for accuracy.
- **Data cleaning protocols:** Consistency checks, logical validation (e.g., impossible values), and cross-timepoint checks are applied systematically.
- **Documentation:** All data transformations, decisions, and corrections are documented in a project log and reflected in the data dictionary.
- **Peer review:** At least one additional team member will review the final cleaned datasets and analytical code to ensure accuracy and methodological integrity.

These procedures collectively ensure a high standard of data accuracy, consistency, and reproducibility throughout the project.

Documentation and Metadata

What documentation and metadata will accompany the data?

Documentation and metadata accompanying the data
Comprehensive documentation will accompany all datasets to ensure that the data can be understood, interpreted, and reused in the future. This includes project-level documentation, dataset-level metadata, and variable-level details. Documentation will describe the study design, data collection procedures, analytical decisions, and any assumptions made during processing.

Information needed for future interpretation
To enable long-term usability, accompanying documentation will include:

- Project title, description, and research objectives
- Names and roles of data creators and contributors
- Data collection timeline (T1–T5)
- Methodology, including instruments used, scoring procedures, and intervention structure
- Definitions of all variables, scales, scoring rules, and units of measurement
- Explanation of dataset structure and file formats (CSV, PDF)
- Notes on missing data, transformations, derived variables, and cleaning procedures
- Conditions for access, reuse, and any restrictions due to GDPR and AU policies
- Version history and change logs

This ensures that future users—within or beyond the project team—can accurately understand and evaluate the data.

How documentation and metadata will be created/captured
Documentation will be maintained in dedicated files within the project's SIF structure, including:

- A **data dictionary** describing each variable, its coding, labels, permissible values, and origin (survey item, diary, etc.)
- A **codebook** summarising datasets, formats, and relationships between files
- A **methodological summary** outlining data-collection procedures, measurement instruments, and intervention workflow
- A **data processing log** documenting cleaning steps, transformations, and analytical decisions
- Embedded metadata in REDCap exports, such as instrument names, branching logic, and field types

Digitised materials (e.g., PDFs) will include basic metadata in the file properties (title, date, participant ID pseudonym, data type).

Metadata standards
Where possible, the project will adhere to widely used social science metadata standards, including elements inspired by the **DDI (Data Documentation Initiative)** framework. This provides structured, machine-readable descriptors for datasets, variables, collection methods, and file formats. Although full DDI implementation is not required, using DDI-aligned elements ensures that the metadata remain compatible with common research data repositories and future archiving needs.

Additionally, REDCap's built-in metadata structures follow established clinical/biomedical data-collection standards (e.g., controlled variable types, audit logs), which further support structured documentation.

Ethics and Legal Compliance

How will you manage any ethical issues?

Consent for data preservation and sharing
Participants provide informed, written consent to take part in the research project, including the collection and long-term preservation of their data for research purposes. In accordance with Danish data-protection law (§10), data processing for scientific research does **not** rely on GDPR consent but is based on legal authority. Nevertheless, the participant information and consent materials transparently describe how data will be stored, for how long, and under what conditions the data may be accessed or reused. Any future sharing of data outside the project team will occur only in anonymised or appropriately aggregated form and in compliance with AU's policies and national regulations.

Protection of participant identity
Participants' identities are protected through strict **pseudonymisation** procedures. Direct identifiers (e.g., names, contact details) are stored separately from research data, linked only through project-specific participant IDs. Access to the identification key is restricted to authorised project staff and stored on AU's secure infrastructure (**SIF**) with role-based access controls. Any datasets prepared for analysis or potential future sharing will be fully anonymised by removing all direct identifiers, indirect identifiers, and any information that could enable re-identification.

Handling and security of sensitive data
All sensitive personal data—including mental health-related questionnaire data, sleep diaries, and intervention materials—are processed and stored within AU's approved secure environments (REDCap and SIF). These systems provide:

- Encrypted data transfer and encrypted storage
- Access control using institutional authentication
- Audit trails and logging of user activity
- Regular backups and disaster-recovery protections
- Secure upload routes for digitised paper materials (PDFs)

No data are stored on personal devices. If paper-based materials are collected (e.g., sleep diaries), they are kept in locked facilities accessible only to authorised staff, then digitised and transferred securely to SIF and destroyed according to protocol.

Ethical review and compliance
The study follows AU's institutional guidelines for responsible data management and has been reviewed according to the local ethical and data-protection procedures applicable to research involving human participants. All data-handling practices comply with the General Data Protection Regulation (GDPR), the Danish Data Protection Act, and AU's internal data-protection policies.

How will you manage copyright and Intellectual Property Rights (IPR) issues?

Ownership of data
All research data generated in the project, including questionnaire responses, sleep diary data, intervention-related materials, and derived datasets, are owned by **Aarhus University** in accordance with institutional policies on research data management and intellectual property. Project staff have access rights for research purposes but do not individually own the data.

Licensing the data for reuse
Because the project involves **sensitive personal data** processed under the Danish Data Protection Act (§10), the raw or pseudonymised datasets **cannot be openly shared**. Any future sharing outside the research group will occur only in **fully anonymised** form and in line with AU policies, GDPR, and ethical approvals. If anonymised data are suitable for reuse, they may be shared under a standard open licence such as **CC BY 4.0** or **CC0**, depending on AU guidelines and the degree of de-identification possible. Licensing decisions will be made upon project completion and only if the anonymisation meets legal and ethical requirements.

Restrictions on third-party data reuse
The project does **not** rely on external or third-party datasets. All data are collected directly from participants or created within the project. Therefore, no third-party IPR or licensing restrictions apply.

Postponed or restricted data sharing
Data sharing may be **restricted or postponed** temporarily to allow sufficient time for:

- Completion of primary analyses
- Publication of findings
- Ensuring that any shared dataset is fully anonymised and GDPR-compliant

No patents are anticipated from this project, and no patent-related delays in data dissemination are expected.

All decisions regarding data sharing will follow AU's research-data policies, the project's ethical approvals, and applicable legal frameworks.

Storage and Backup

How will the data be stored and backed up during the research?

Storage infrastructure and capacity
All research data will be stored on **Aarhus University's secure IT infrastructure**, specifically **REDCap** (for active data collection) and **SIF** (AU's Secure Research Platform) for storage, processing, and analysis. Both systems are designed for handling sensitive personal data and provide sufficient capacity for the project's needs. No additional storage costs are expected, as the data volume is modest and well within AU's existing allocations.

Backup procedures
Backups are handled automatically by AU IT Services for both REDCap and SIF. These systems use redundant storage, institutional-level backup routines, and regular snapshots to protect against accidental loss, corruption, or system failure. Backups occur daily (or more frequently depending on system policies) and are stored within AU's secure infrastructure.

No data will be stored locally on laptops, portable devices, or external drives. Any paper-based materials (e.g., sleep diaries) will be digitised and transferred to SIF as soon as possible; the digital copies then fall under standard AU backup procedures.

Responsibility for backups and recovery
Backup and recovery of the underlying systems (REDCap and SIF) are the responsibility of **Aarhus University IT Services**, which manages system maintenance, monitoring, and disaster

recovery. The research team is responsible for ensuring that all project data are stored exclusively within these approved environments and for verifying that data exports, processed files, and documentation follow the project's defined file structure on SIF.

Recovery in case of an incident

In the event of an incident such as accidental deletion, system failure, or data corruption, AU IT Services can restore data from server-level backups or system snapshots. The project team will document any incidents, verify the integrity of restored data, and reintroduce any necessary analysis scripts or documentation from the most recent backed-up version. Because all data are stored on centrally managed services with built-in redundancy, the risk of unrecoverable data loss is low.

How will you manage access and security?

Risks to data security and how they will be managed

The primary security risks relate to the handling of **sensitive personal data**, including unauthorised access, accidental disclosure, data loss, or processing outside approved systems. These risks are managed by storing all data exclusively within **Aarhus University's secure infrastructure** (REDCap and SIF), which complies with institutional data-protection requirements and follows recognised information-security principles consistent with ISO 27001. Additional technical and organisational measures—including encryption, access control, audit logs, and secure authentication—significantly reduce the likelihood of security incidents.

Access control measures

Access to data is restricted to authorised members of the research team based on the principle of **least privilege**.

- Access to REDCap is managed through AU's central authentication (WAYF/AU ID), with role-based permissions.
- Access to SIF is controlled via individual user accounts, two-factor authentication, and explicit approval from AU IT.
- Identifiable participant information is stored separately from research datasets, linked only through pseudonymised participant IDs.
- All access, modifications, and downloads are logged through system-level audit trails.

No data are stored on personal devices, email accounts, consumer cloud services, or unencrypted storage media.

Secure access for collaborators

If collaborators require access, they will be granted **role-appropriate user rights** within SIF or REDCap, following AU's procedures for secure onboarding. External collaborators (if applicable) must use AU-approved secure access methods and agree to AU's data-protection terms. Data will never be transferred by email, USB stick, or other unsecured channels. Instead, all collaboration occurs within controlled, institutional environments.

Safe transfer of field-collected data

Field data collection for this project primarily involves REDCap surveys and digitised sleep diaries.

- **Electronic data** are entered directly into REDCap, eliminating local storage and reducing transfer risk.
- **Paper-based materials** (e.g., sleep diaries) are temporarily stored in locked, access-restricted facilities. They are then digitised and transferred directly into SIF using secure AU-managed devices, after which the paper originals are stored securely or destroyed according to protocol.
- No sensitive data are transported on personal devices or stored outside AU's secure systems at any time.

These measures ensure that all data—whether collected digitally or on paper—are securely transferred into the main protected environment without exposure to unnecessary risk.

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

Data required to be retained or destroyed for legal or regulatory purposes

Because the project processes **sensitive personal data** under the Danish Data Protection Act (§10 for research), all identifiable data must be stored, handled, and eventually destroyed according to AU's data-protection rules and institutional retention policies. Identifiable data (e.g., consent forms, contact information, identification keys linking participant IDs to identities) will be retained only for as long as necessary to complete the research and ensure data integrity. Once the project is completed and all analyses are finalised, identifiable data will be securely destroyed in accordance with AU and GDPR requirements. Pseudonymised or anonymised research data may be retained for longer to support transparency, auditability, and reproducible research.

Criteria for deciding what other data to keep

Decisions about long-term retention will prioritise datasets that:

- Are essential for **replication** or validation of published results
- Are sufficiently **anonymised** to allow safe long-term retention
- Have **future scientific value**, such as enabling meta-analyses or follow-up research
- Are feasible to preserve without compromising participant privacy or violating GDPR principles

Working files, temporary data extracts, intermediate analysis outputs, and materials containing identifiers will not be preserved.

Foreseeable future research uses

Anonymised datasets may be useful for:

- Verification of the study's findings
- Secondary analyses or methodological research
- Integration into larger datasets for meta-analysis or comparative studies
- Pedagogical purposes (e.g., teaching research methods), provided full anonymisation is achieved

Any reuse will occur strictly in anonymised form and in accordance with AU policies and legal requirements.

Length of retention and preservation

In line with AU's guidelines for research data management, anonymised research datasets of long-term value may be preserved for **a minimum of 5 years after project completion**, or longer if they support ongoing or future research. Identifiable data will be retained only for the time legally permitted and operationally required, after which they will be securely destroyed.

Data selected for long-term preservation will be stored in durable formats (e.g., CSV and PDF/A) to ensure accessibility and compatibility with future technologies.

What is the long-term preservation plan for the dataset?

Repository or archive for long-term preservation

Anonymised datasets deemed to have long-term scientific value will be preserved in **Aarhus University's institutional research data archive** or another AU-approved secure repository suitable for long-term preservation. These repositories provide controlled access, robust metadata support, long-term storage stability, and compliance with GDPR and Danish research-data regulations. Sensitive data will *not* be deposited in open repositories unless fully anonymised to a level that guarantees non-identifiability.

Fully anonymised datasets may also be deposited in an appropriate national or discipline-specific archive (e.g., the **Danish National Archives**, if relevant), provided they meet the archive's anonymisation and metadata requirements.

Costs associated with preservation

Aarhus University's institutional storage and long-term preservation services are expected to cover the project's needs without additional cost. No external repository fees are anticipated. If future sharing in a national archive requires minor administrative costs (e.g., metadata formatting), these are expected to be minimal and manageable within existing project resources.

Preparation and documentation effort

Time and effort for preparing data for long-term preservation—such as anonymising datasets, preparing metadata, updating codebooks, and documenting methods—have been built into the project workflow.

This includes:

- Producing a final, fully anonymised version of the dataset in durable formats (e.g., CSV, PDF/A)
- Preparing the accompanying documentation (metadata, codebook, variable descriptions, methodological notes)

- Conducting a final quality and consistency review
- Ensuring that all identifiers and indirect identifiers are removed or masked
- Archiving the dataset along with persistent metadata and licensing information

These steps ensure that the dataset is complete, compliant, and interpretable beyond the lifetime of the grant.

Post-project curation

After project completion, the archived dataset will remain stored in the selected institutional or national repository according to AU's retention guidelines. Access will be restricted and governed by the repository's policies, ensuring continued protection of participant privacy while enabling legitimate scientific reuse.

Data Sharing

How will you share the data?

How users will learn about the data

If anonymised data are suitable for sharing, the availability of the dataset will be communicated through:

- Citations in publications resulting from the project
- Depositing metadata records in an AU-approved repository, enabling external researchers to discover the dataset
- Documentation in the project's final report and on institutional platforms where appropriate

These metadata records will clearly describe the dataset, its scope, anonymisation level, and access conditions.

With whom the data will be shared and under what conditions

Due to the sensitive nature of the original data, **only fully anonymised datasets** will be shared, and only when it is legally and ethically permissible. Data may be shared with qualified researchers or research groups for legitimate scientific purposes, subject to:

- Sufficient anonymisation to meet GDPR and AU standards
- Approval by the repository or institutional data access committee (if applicable)
- Users agreeing to acknowledge the dataset appropriately and comply with reuse conditions

Identifiable or pseudonymised data will *not* be shared outside the project team.

Mechanism for sharing

Anonymised datasets will be shared either through:

- An AU-approved institutional repository with controlled access, or
- A national secure archive (e.g., the Danish National Archives), where access is governed by formal application procedures

Direct sharing by the research team will only occur through secure, institutionally approved channels and only when appropriate agreements (e.g., data use agreements) are in place.

Timing of data availability

Data will be made available **after project completion** and after:

- Final analyses and publications have been completed
- The dataset has been fully anonymised
- Accompanying documentation (metadata, codebook, methods) has been prepared and validated

This ensures that data released is accurate, complete, and interpretable.

Persistent identifier

If the data are archived in an institutional or national repository, a **persistent identifier** (such as a DOI) will be requested. This ensures that the dataset is citable, traceable, and discoverable. Users will be encouraged to cite the dataset in any publications arising from its reuse.

Are any restrictions on data sharing required?

Restrictions and their causes

Restrictions on data sharing are primarily due to the presence of **sensitive personal data**, which fall under GDPR and the Danish Data Protection Act (§10 for research). These legal and ethical constraints mean that identifiable or pseudonymised data **cannot** be shared outside the project team. Only fully anonymised datasets—after thorough assessment to ensure no risk of re-identification—may be shared.

Additional restrictions may arise if free-text responses or small subgroups make complete anonymisation challenging.

Actions to overcome or minimise restrictions

To enable some form of sharing while protecting participants, the project will:

- Produce a **fully anonymised dataset**, removing all direct and indirect identifiers
- Aggregate or suppress variables where anonymisation is otherwise insufficient
- Provide detailed metadata and documentation to improve usability of the anonymised dataset
- Use institutional or national repositories with **controlled access** to ensure secure dissemination
  These steps balance research transparency with legal and ethical obligations.

Exclusive use period

The research team will require exclusive use of the data until:

1. All primary analyses are completed,
2. Planned publications derived from the project are submitted or published, and
3. Anonymisation has been fully implemented and validated.
   This ensures the project team has adequate time to analyse the data and disseminate findings before sharing occurs.

Need for data sharing agreements

If sharing is requested for legitimate research purposes, and only after anonymisation has been achieved, a **data sharing agreement** (DSA) or equivalent may be required. The DSA would outline:

- Permitted uses of the anonymised dataset
- Obligations to protect participant confidentiality
- Prohibitions on attempting re-identification
- Requirements for secure handling and proper citation
  For more sensitive derived materials or limited-access metadata, a controlled-access repository may instead require a formal application or institutional approval.

Responsibilities and Resources

Who will be responsible for data management?

The **Principal Investigator (PI)** (ph.d.-student Alexander Castro-Pavlik) is responsible for the implementation of the Data Management Plan (DMP), ensuring that it is followed throughout the project and reviewed or updated as needed. The PI also ensures that all research activities comply with Aarhus University's research data policies, ethical guidelines, and relevant GDPR requirements.

Responsibilities for specific data management activities

- **Data capture and collection:**
  Conducted by the project's research team and clinical staff, who are responsible for entering and verifying data in REDCap, ensuring adherence to standardised procedures.
- **Metadata creation and documentation:**
  Led by the PI or a designated data manager/research assistant, who will maintain data dictionaries, codebooks, processing logs, and methodological documentation.
- **Data quality control:**
  Shared between the PI and designated research staff. Responsibilities include implementing validation rules in REDCap, reviewing digitised materials, performing routine data checks, and documenting data cleaning processes.
- **Storage and backup:**
  Managed by **Aarhus University IT Services**, who maintain REDCap and SIF, including automated backups, secure access control, and disaster recovery procedures. The research team is responsible for ensuring that all data are stored exclusively within these approved environments.
- **Data security and access control:**
  Overseen by the PI, who ensures that only authorised team members are granted role-appropriate access to REDCap and SIF. AU IT Services manage the technical access controls, authentication, and system-level logging.
- **Data archiving and long-term preservation:**
  The PI or designated data steward is responsible for preparing anonymised datasets and accompanying documentation for deposit in an approved repository or archive, following AU's retention and preservation requirements.
- **Data sharing:**
  The PI oversees all external data-sharing decisions to ensure compliance with GDPR, ethical approvals, and institutional guidelines. Any sharing will be conducted only through AU-approved secure channels or repositories.

Collaborative responsibilities (if applicable)
If the project engages external collaborators, data management responsibilities will be defined in collaboration agreements. These agreements will specify data access rights, responsibilities for analysis, sharing conditions, and obligations to follow AU's data protection and security guidelines. Data ownership will remain with **Aarhus University**, unless otherwise defined in such agreements.

However, no engagement of external collaborators have been planned in this study.

What resources will you require to deliver your plan?

Specialist expertise and training
The project does not require dedicated data management personnel beyond the existing research team. All staff involved in data collection and handling will receive training in:

- Use of **REDCap** for secure data capture
- Use of **SIF** for secure storage and analysis of sensitive data
- GDPR compliance and AU's data-protection procedures
- Standardised data entry, documentation, and file management practices

In relation to **clinical data collection**, all therapists delivering the intervention are either already trained specialists (Alexander D. Castro-Pavlik) in **behavioural sleep treatment** or will receive extensive training from recognised specialists prior to conducting treatment (Alexander D. Castro-Pavlik, associate prof. Ali Amidi at Aarhus University). Throughout the entire intervention period, these specialists will provide **continuous supervision** to ensure treatment fidelity, adherence to protocol, and consistent, high-quality data collection.

No additional external expertise beyond this structured clinical training and supervision is anticipated.

Hardware and software requirements
The project relies on institutional systems already provided by Aarhus University, including:

- **REDCap** for structured data collection
- **SIF** for secure storage, processing, and long-term preservation
- Standard AU-licensed statistical software (e.g., R, SPSS, Stata, Python)
- AU-managed scanning equipment for digitising paper-based materials such as sleep diaries

No additional or exceptional hardware or software is required. Sensitive data will not be stored on personal devices.

Repository or archiving costs
No repository fees are expected. Long-term preservation will use AU's institutional repository or another AU-approved archive, typically at no cost. Any minor administrative work required for national repositories (if used) can be absorbed within existing project resources.

Overall resource sufficiency
AU's existing digital infrastructure provides all necessary secure services for data capture, processing, storage, and preservation. Combined with the specialist training and supervision of therapists, the project has sufficient resources and institutional support to fully implement the Data Management Plan.