**DDP-Bildung**

**Mindestanforderung III.a):  
Sichern von (Meta-)Daten**

**III. Themenbereich: Sichern im Projekt**

# Versionierungshistorie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | | Typ | Datum | erstellende Person |
| 1 | 20200508 | erster Entwurf | 08.05.2020 | sen |
|  |  | Review | 13.05.2020 | mk/ ap/ jks |
| 2 | 20200515 | überarbeitete Version | 15.05.2020 | sen |
|  |  | Kommentiert | 20.05.2020 | gf |
| 3 | 20200610 | MA überarbeitet & Stichpunktsammlung entfernt | 10.06.2020 | sen |
| 4 | 20200721 | Abschnitt D ergänzt | 21.07.2020 | sen |
| 5 | 20201124 | MA überarbeitet | 24.11.2020 | sen |
| 6 | 20201125 | Version für RDMO | 25.11.2020 | sen |

# Mindestanforderung

Daten, zugehörige Metadaten und Begleitmaterialen werden im Projektverlauf systematisch gespeichert, in einem zentralen, zugriffsgeschützten Back-Up-System gesichert und ihre Nutzbarkeit kontinuierlich überprüft.

## Abhängigkeiten mit anderen Modulen

Diese Mindestanforderung steht in Verbindung zu folgenden weiteren DDP-Modulen:

I.a) Berücksichtigung existierender Daten,

III.b) Schutz personenbezogener und sensibler Daten im Projekt,

IV.b) rechtlichen Vorgaben des Datenschutzes im Umgang mit personenbezogenen Daten,

V.b) Langfristsicherung von Daten.

[ggf. WEITERE MODULE ERGÄNZEN]

## Erörterungen zur Mindestanforderung

1. Die Mindestanforderung fordert ein für das jeweilige Forschungsprojekt geeignetes Speichern der Daten, ihrer Metadaten sowie weiterer Begleitmaterialien; dies betrifft u.a.
   1. unterschiedliche Speichermöglichkeiten, wie auf dem lokalen Rechner, auf portablen Speichermedien, wie USB-Sticks, CDs etc., in Cloud-Systemen oder Netzwerken,
   2. unterschiedliche Speichermedien, wie z. B. magnetische Speichermedien oder Flashdrives (siehe *Standards* und *weiterführende Ressourcen* dieses DDP-Moduls) ebenso wie
   3. die Dateiformate in denen Daten und Begleitmaterialien gespeichert werden sowie die notwendige Software zur Nutzung der Daten.

Bei der Wahl geeigneter Speichermöglichkeiten und –medien sind die Möglichkeiten und Vorgaben der Institute der Forschenden ebenso zu beachten wie die benötigte Speicherkapazität, z. B. mit Blick auf die Größe der zu speichernden Daten und Dateien.

1. Voraussetzung zur Sicherung der Daten, ihrer Metadaten sowie weiterer Begleitmaterialien ist eine adäquate Organisation der Dateien im Forschungsprojekt (siehe hierzu auch die weiteren DDP-Elemente dieses Moduls); dies betrifft u. a.
   1. den Aufbau und die konsistente Nutzung einer für das jeweilige Forschungsprojekt angemessenen Ordnerstruktur,
   2. die einheitliche und konsistente Benennung von Dateien sowie
   3. deren einheitliche und konsistente Versionierung über dem gesamten Projektverlauf hinweg.
2. Die Mindestanforderung fordert auch das systematische Erstellen von Sicherungskopien der Daten, ihrer Metadaten sowie weiterer relevanter Dateien zum Schutz vor Verlust, versehentlichem Löschen, Überschreiben etc., d. h. der Implementierung und konsistenten Umsetzung einer für das Forschungsprojekt geeigneten Back-Up-Strategie:
   1. Zur Gewährleistung einer geeigneten Back-Up-Strategie können Forschende
   * auf institutionelle Verfahren und Richtlinien zurückgreifen,
   * sich der Back-Up-Verfahren von entsprechenden Cloud-Diensten zur Speicherung von Daten und Dateien bedienen,
   * bereits im laufenden Projekt als Back-Ups an ein Repositorium übergeben (und ggf. mit einem zeitlichen Embargo bis zum Ende der Projektlaufzeit versehen) oder
   * eine eigene Back-Up-Strategie entwickeln, implementieren sowie konsistent umsetzen und dokumentieren (siehe *Standards* und *weiterführende Ressourcen* des vorliegenden DDP-Moduls).

Die Nutzung institutioneller Back-Up-Prozesse bzw. von Cloud-Diensten oder die Übergabe der Back-Ups während der Projektlaufzeit an ein Repositorium setzen die Kenntnis entsprechender Sicherungsprozesse bei den Forschenden voraus. Insbesondere ist darauf zu achten, dass die Dateien regelmäßig gesichert werden, dass ausreichend Sicherungskopien erstellt werden und entsprechend Speicherkapazität verfügbar ist, dass mindestens eine Back-Up-Version extern gespeichert wird und dass die Forschenden Zugang zu den Sicherungskopien haben (siehe hierzu auch *Standards* und *weiterführende Ressourcen* des vorliegenden DDP-Moduls).

* 1. Die Speicherung und Back-Up-Strategie umfassen auch die Sicherung relevanter Informationen in Papierformat, wie etwa (handschriftlich) ausgefüllte Fragebögen, handschriftliche Notizen von Interviewer\*innen oder die unterschriebenen Einwilligungserklärungen. Diese sollten nach Möglichkeit digitalisiert und in die digitalen Back-Ups integriert werden oder zumindest in Kopie extern gesichert werden.
  2. Die erstellten Sicherungskopien müssen mindestens einmalig nach ihrem Erstellen auf ihre Funktionalität hin überprüft und mit den Ausgangsdateien verglichen werden (Datenintegrität), um zu gewährleisten, dass keine relevanten Daten, Metadaten und weitere relevante Informationen verloren gehen. Dies betrifft auch die Back-Ups der Daten, Metadaten und Begleitmaterialien, die zu Projektende in die Langristsicherung gehen (siehe hierzu auch *Standards* und *weiterführende Ressourcen* des vorliegenden DDP-Moduls ebenso wie Modul V.b) *Langfristsicherung von Daten*).

1. Bei sämtlichen Speicheraktivitäten und Back-Up-Maßnahmen sind alle datenschutzrechtlich relevanten Vorgaben zu beachten und einzuhalten (siehe hierzu DDP-Modul III.b) zum *Schutz personenbezogener und sensibler Daten im* *Projekt* sowie DDP-Modul IV.a) zu den *rechtlichen Vorgaben des Datenschutzes* im Umgang mit personenbezogenen Daten).
2. Das Sichern von Daten und Begleitmaterialien im Rahmen des Forschungsprojekts schließt auch deren projektbegleitende Löschung bzw. Vernichtung mit ein, wenn diese nicht weiter benötigt werden. Gerade mit Blick auf personenbezogene Informationen und Daten von Dritten, wie z. B. Behörden, sind dabei rechtliche Vorschriften, Lizenzbedingungen und sonstige Vorgaben der Datengebenden zu beachten (siehe hierzu auch *Standards* und *weiterführende Ressourcen* des vorliegenden DDP-Moduls sowie DDP-Modul I.a) zur *Berücksichtigung bereits existierender Daten*, DDP-Modul III.b) zum *Schutz personenbezogener Daten* im Projekt und DDP-Modul IV.c) zu den *weiteren rechtlichen und ethischen Regelungen*).
3. Forschende müssen jederzeit dazu in der Lage sein, ihre institutionellen Regelungen zu Speichermöglichkeiten, Back-Up-Verfahren, Verfahrensweisen des eigenen Instituts, von genutzten Repositorien oder Cloud-Systeme bzw. ihre eigene Back-Up-Strategie offen zu legen.
4. Bei Forschungskooperationen (mit Partner\*innen außerhalb der eigenen Institution bzw. außerhalb des eigenen Netzwerks) müssen die Speichermöglichkeiten und -medien ebenso wie die Back-Up-Strategie klar abgesprochen sowie entsprechende Verantwortlichkeiten, Verfahren und Regeln verschriftlicht und allen Beteiligten (dauerhaft) zugänglich gemacht werden.
5. Werden die Daten durch Dritte erhoben, z. B. durch ein Erhebungsinstitut, dann ist die Übermittlung der Daten an die Forschenden ebenso wie deren Zugang, Sicherung und Löschung beim Erhebungsinstitut schriftlich zu regeln (siehe hierzu auch die *Anwendungsfälle* und *Standards* des vorliegenden DDP-Moduls sowie DDP-Modul III.b) zum *Schutz personenbezogener Daten* im Projekt und DDP-Modul IV.a) zu *rechtlichen Aspekten des Datenschutzes*).