Hinweise zum Formular Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO

- **Bezeichnung**
  Hier ist die (interne) Bezeichnung des Verfahrens anzugeben (z.B. Projekt xy – Auswertung der Fragebögen).
- **Erstmeldung / Änderungsmeldung / Auflösungsmeldung**
  Erstmeldung: Datum, an dem das Verarbeitungsverzeichnis das erste Mal abgegeben wird.
  Änderungsmeldung: Nur relevant wenn das Verarbeitungsverzeichnis eine vorherige Meldung ersetzt (bleibt leer bei Erstmeldung).
  Auflösungsmeldung: Mitteilung, dass das Verfahren aufgegeben wurde (bleibt leer bei Erstmeldung und/oder Änderungsmeldung).
- **Einführungsdatum und Änderungsdatum**
  Einführungsdatum: Datum, an dem das System aktiviert werden soll.
  Änderungsdatum: Datum, an die Änderung am System vorgenommen wird.

1. Verantwortliche Stelle an der HU (Verfahrensverantwortliche_r)

- Tragen Sie hier bitte die Bezeichnung und Anschrift Ihres Arbeitsbereichs und den Namen der Leiterin / des Leiters ein. (z.B. LS xy Prof. xy).

- Es sind Bezeichnung und Anschrift Ihres Arbeitsbereichs und der Name der Leiterin / des Leiters einzutragen.

2. Eingesetzte / s Software / Verfahren

- **Betriebsart:** Beispiel: Dialog- oder Stapelverarbeitung, relationale Datenbank, Telekommunikations- oder Prozessteuerungssystem, Einzelplatzrechner, vernetzte Rechner.

- **Art der Geräte:** Tragen Sie bitte hier die zur Datenübermittlung verwendeten Geräte mit deren Inventar-Nummer ein. Beispiel: Server, PC-Arbeitsplätze, Laptop, Ausgabegeräte (Drucker, Fax), Laufwerke.

- **Aufstellung der Geräte in folgender Organisationseinheit / Stelle:**

- **Verfahren der Übermittlung, Sperrung, Löschung, Auskunftserteilung:** Hierbei handelt es sich um Rechte, die Betroffenen zustehen. Tragen Sie hier bitte ein, wie diese Rechte im Bedarfsfall umgesetzt würden:

  - **Übermittlung:** z.B. Bereitstellung über Schnittstelle (verschlüsselt/unverschlüsselt), Übergabe eines Ausdrucks, …. durch Arbeitsgruppe xy

  - **Sperrung:** z.B. Setzen eines Merkmals innerhalb der Datei oder Entfernung in Verbindung mit Archivierung auf einem externen Datenträger (CD).

  - **Löschung:** z.B. Vernichten von Datenträgern (Entsorgungsprotokoll); sicheres Überschreiben.

  - **Auskunftserteilung:** z.B. mündliche Auskunft, Ausdruck des Datensatzes; durch Mitarbeiter des Servicedesktops; durch Projektleiter (Anschrift).

3. Datenverarbeitung

a) Zwecke (vgl. Art. 5 Abs. 1 b) DSGVO): Der Zweck der Datenverarbeitung ist so präzise wie möglich zu benennen. (z.B. Verwaltung der personenbezogenen Daten im Zusammenhang mit der Vergabe von Seminarräumen). Die Zweckbestimmung ist sorgfältig zu treffen. Sie steht in engem Zusammenhang mit der Rechtsgrundlage und begrenzt dauerhaft die Anwendungsgebiete, für welche die Daten genutzt werden dürfen. Andererseits ist eine zu weite Zweckbestimmung unzulässig.

b) Rechtsgrundlage (vgl. Art 6 Abs. 1 DSGVO): Anzugeben ist die konkrete Rechtsvorschrift inkl. Paragraphen-/Artikelnennung. Anmerkung: Die Verarbeitung von Daten im Rahmen von Forschungsprojekten erfolgt häufig aufgrund einer Einwilligung. Hinweise zur Gestaltung einer wirksamen informierten Einwilligung sind auf www.hu-berlin.de/datenschutz oder bei der behördlichen Datenschutzbeauftragten (behDSB) zu finden.

4. Auftragsverarbeitung

Eine solche kommt nur in Frage, wenn externe Dienstleister in die Datenverarbeitung eingebunden sind *[Liegt keine Auftragsverarbeitung vor, bitte bei 5) fortfahren].*

- Auftragsverarbeitungsvertrag vom *(Datum des Vertragsabschlusses)*
- Gegenstand und Dauer der Auftragsdatenverarbeitung *(Hier ist der Zweck und die Dauer anzugeben)*.

a) Auftragsverarbeiter

Bitte die Angaben des externen Dienstleisters eintragen.

b) Auftragsverarbeiter

Bestehen geeignete Verhaltensregeln, Garantien oder Zertifizierungsverfahren (vgl. Art. 40 DSGVO, Art. 42 DSGVO).

- Genehmigte Verhaltensregeln nach Art. 40 DSGVO
- Genehmigtes Zertifizierungsverfahren nach Art. 42 DSGVO
- Garantien für geeignete technische und organisatorische Maßnahmen

c) durch den Auftragsverarbeiter ggf. eingeschaltete Subunternehmer

[Auszufüllen, soweit der Auftragnehmer Subunternehmer (z.B. Internet-Hoster) einsetzt].

5. Beschreibung der Kategorien betroffener Personen

Betroffene sind die Menschen, deren personenbezogene Daten verarbeitet werden. Der Kreis der Betroffenen ist möglichst präzise zu bezeichnen. Bsp.: Studenten des Kurses xx, Lehrstuhl für xy, Mitarbeiter der Abteilung xy etc.).

6. Beschreibung

a) der personenbezogenen Daten oder Datenkategorien:

z. B. Name, Vorname, Geburtsdatum, Antworten zu Testfragen zu den Themenfeldern xy, etc.

b) der besonderen Arten personenbezogener Daten oder Datenkategorien:

Nach Art. 9 Abs. 1 DSGVO: personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

7. Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden

Wer erhält die Daten außerhalb Ihrer Einrichtung (= außerhalb der unter 1. genannten Stelle)?

a) Intern: Dateiübermittlungen innerhalb der Universität.

b) Extern: Dateiübermittlungen an andere Stellen (z.B. Drittmittelgeber)

c) Drittland oder internationale Organisation: (vgl. Art. 44 ff. DSGVO) tragen Sie hier bitte die Kategorie Drittland oder internationale Organisation ein, sofern zutreffend.

- Drittland: Land außerhalb der Europäischen Union
- oder an eine internationale Organisation

8. Datenübermittlung an ein Drittland oder eine internationale Organisation

[Nur bei Übermittlung personenbezogener Daten an Stellen außerhalb der Europäischen Union auszufüllen]. Tragen Sie bitte den/die Empfänger der personenbezogenen Daten hier ein.

- Drittland: Land außerhalb der Europäischen Union
- internationale Organisation (vgl. Art. 44 ff. DSGVO).

a)

Angaben ob eine Datenübermittlung stattfindet oder nicht, Name des Drittlandes oder Name der internationalen Organisation, die Namen der konkreten Datenempfänger.

b)

- Bitte ankreuzen sofern ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO für das Empfängerland vorliegt. Eine jeweils aktuelle Übersicht zu diesen Beschlüssen ist auf den Seiten der EU-Kommission zu unter der Adresse https://ec.europa.eu/info/law/law-topic/data-protection_de zu finden.

- Gibt es geeignete Garantien nach Art. 46 DSGVO? Bezeichnung, z.B. in Anlage

- Liegt eine nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung vor? Dokumentation z.B. in Anlage

9. Herkunft bzw. Quelle empfangener Daten

Hier sind nur Angaben zu machen, wenn Sie regelmäßig Daten von Dritten erhalten. Es sind die Datenquellen (z.B. Einwohnermeldeamt) anzugeben, von der die Einzeldaten regelmäßig bezogen oder direkt erhoben werden.

10. Zugriffsberechtigte Personen oder Personengruppen (aufgeteilt nach Art der Berechtigung, z.B. Lese-, Schreibberechtigung)

Geben Sie bitte alle Personen an, die Zugriff auf die Daten haben. Differenzieren Sie bitte dabei: Wer darf was? Welche Personen dürfen Daten erheben, speichern, verändern, übermitteln, sperren, löschen und nutzen? Sofern unterschiedliche zugriffsberechtigte Mitarbeiter auf unterschiedliche Datenkategorien (siehe Punkt 6 a)) zugreifen können, sollte auch dies erkennbar sein. Grenzen Sie die Gruppen bitte ein. Also nicht: "Mitarbeiter der xy-Abteilung", wenn nur eine bestimmte Arbeitsgruppe gemeint ist. Konkrete Namen müssen hingegen nicht genannt werden, die Stellenbezeichnung ist ausreichend.

11. Fristen für die Sperrung und Löschung der Daten

Vor Beginn der Verarbeitung (erstmalige Verarbeitung) ist festzulegen, wann welche Datenarten zu sperren oder zu löschen sind.

a) Sperrung: Kennzeichnung der Daten, die bewirkt, dass diese nicht mehr aufgerufen/verarbeitet werden können.

b) Löschungen: Endgültiges Beseitigen der Daten.

Aufbewahrungsfristen können sich aus Gesetzen, z.B. aus der StudDatenVO ergeben. Ansonsten ergeben sich Fristen teils aus dem Verfahren nach Erforderlichkeitserwägungen (z.B. Ablauf von Widerspruchsfristen) oder z.B. dem Ende von Nachweispflichten. Im Zweifel können Sie bei den behDSB nachfragen.

12. Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO

Hinweis: Komplexe Datenverarbeitungsvorgänge oder Vorgänge mit sensiblen Daten erfordern ein gesondertes, ausführliches Sicherheitskonzept (SiKo) samt Risikoanalyse. Die zentralen Maßnahmen sind hier einzutragen. Sofern es für Ihre Anwendung kein SiKo gibt, nehmen Sie im Zweifel bitte Rücksprache mit den behDSB.

a) Pseudonymisierung und/oder Verschlüsselung personenbezogener Daten

vgl. Art. 32 Abs. 1 a) DSGVO

- **Pseudonymisierung** vgl. Art. 4 Nr. 5 DSGVO: die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

b) Vertraulichkeit, Integrität, Verfügbarkeit (einschließlich Wiederherstellung) und Belastbarkeit der Systeme und Dienste:

Hier sind die konkreten Maßnahmen zu beschreiben, durch welche die Sicherheit der Datenverarbeitung gewährleistet wird (Art. 32 Abs. 1 a) DSGVO).

- **Vertraulichkeit:** Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden. *Bsp.: Daten mit unterschiedlicher Zweckbindung werden getrennt verarbeitet, hardware- und wissensbasierte Zugriffskontrolle (Türen, Chipkarten, Passwörter), Einsatz von Verschlüsselung.*

- **Integrität:** Personenbezogene Daten müssen stets unversehrt, vollständig, gültig und widerspruchsfrei bleiben. Schutz der Daten vor (unerlaubter) Veränderung. *Bsp.: Signatur, Verschlüsselung.*

- **Verfügbarkeit:** Daten müssen (in angemessener Zeit) Berechtigten zur Verfügung stehen. Daten sind durch technische und organisatorische Maßnahmen gegen zufällige Zerstörung oder Verlust zu schützen. Hierzu zählen Datensicherungskonzepte/Backups und redundante Systeme.

c) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:

vgl. Art. 32 Abs. 1 d) DSGVO.

d) Authentizität, Revisionsfähigkeit:

- Bestimmbarkeit der Herkunft der Daten, z.B. signierte Daten, Zusatzinformationen

- Nachhaltbare Dokumentation von Änderungen (wer, wann, welche) z.B. Dokumentation, Verfahrensbeschreibung, Protokollierung.

e) Transparenz, Information der Betroffenen:

Nachvollziehbare Dokumentation der Verarbeitung.

- Protokollierung

- Sicherstellung der Auskunftsrechte von Betroffenen
- Ggf. Entsprechende Information des Betroffenen (frühzeitig und unaufgefordert)

f) Sonstiges

13. Sonstiges / Referenzdokumente

hier ist jeweils das Datum und die Anlagebezeichnung einzutragen

- Datensicherheitskonzept (SiKo) und Risikoanalyse

  Komplexe Datenverarbeitungsvorgänge oder Vorgänge mit sensiblen Daten erfordern ein gesondertes, ausführliches Sicherheitskonzept samt Risikoanalyse. Ob ein erweitertes SiKo erforderlich ist, besprechen Sie bitte mit den behDSB.

  - Im gesonderten SiKo sind die konkreten Maßnahmen zu beschreiben, durch welche die Sicherheit der Datenverarbeitung gewährleistet wird.
  - In der Risikoanalyse nach Art. 24, 32 Abs. 2 DSGVO die Ermittlung der erforderlichen technischen und organisatorischen Maßnahmen anhand der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

- Datenschutzkonzept
- Übersichtliche Darstellung der Verarbeitung
- Muster der Einwilligungserklärung

  Hinweise zur informierten Einwilligung gemäß Art. 13 DSGVO sind auf unter der Adresse https://www.hu-berlin.de/de/datenschutz/einwilligung zu finden.

- Verhaltensregeln
- Datenschutz-Folgenabschätzung (DSFA)

  Nur relevant, wenn eine nach Art. 35 DSGVO vorgeschriebene DSFA stattgefunden hat/erforderlich ist. Dies ist immer dann der Fall, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Eine DSFA ist insbesondere dann durchzuführen, wenn gem. Art. 35 Abs. 3 DSGVO systematische und umfassende Bewertung persönlicher Aspekte oder eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO erfolgt (siehe 6 b). Sowie bei systematischer und umfangreicher Überwachung öffentlich zugänglicher Bereiche. In diesem Fall bitte vorab und frühzeitig Kontakt mit den behDSB aufnehmen.

- Auftragsverarbeitungsvertrag
- Sonstige