Arbeitshilfe Verzeichnis der Verarbeitungstätigkeit

Laut Artikel 30 Abs. 1 der DSGVO hat jede/ jeder Verantwortliche ein Verzeichnis der Verarbeitungstätigkeiten von personenbezogenen Daten, die ihrer Zuständigkeit unterliegen, zu führen und aktuell zu halten. In dem Verzeichnis ist u. a. zu dokumentieren, welche personenbezogenen Daten auf welcher Grundlage und auf welche Art verarbeitet werden und welche technischen und organisatorischen Maßnahmen getroffen werden, um den Datenschutz und die Datensicherheit zu gewährleisten.

Der erste Absatz sowie die kursiven Angaben haben lediglich Hinweis- bzw. Beispielcharakter. Sie sind bei der Bearbeitung zu entfernen. Bei weiteren Fragen kontaktieren Sie bitte Ihre/Ihren Datenschutzbeauftragte/n.

Das Verfahrensverzeichnis gliedert sich in drei Abschnitte: Verantwortliche, Verarbeitungstätigkeit sowie technische und organisatorische Maßnahmen.

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO

Verantwortliche

a) Namen und Kontaktdaten des Verantwortlichen, des Vertreters der Verantwortlichen und des Datenschutzbeauftragten
Die/der Verantwortliche im Sinne der DSGVO ist in der Regel die Leitung der Forschungseinrichtung (in einer Universität in der Regel das Präsidium oder Rektorat, je nach Organisationstruktur). Zusätzlich kann man Prozesseigner bzw. fachlich Verantwortliche, die für die Datenverarbeitungsprozesse in ihrem Bereich zuständig sind, benennen. Gemeint sind damit die Personen, die einen Datenverarbeitungsprozess veranlassen oder leiten - also häufig Abteilungsleitung, Projektleitung o. Ä.

b) Angaben zu einem ggf. gemeinsamen Verantwortlichen:
Nur erforderlich, wenn es gemeinsam Verantwortliche i. S. d. Art. 26 DSGVO gibt, z. B. bei Kooperationen, bei denen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Die/der dazu gehörige rechtliche Vertreter/in ist hier ebenfalls anzugeben. Falls nichtzutreffend, Text bitte löschen.

c) Angaben zum behördlichen Datenschutzbeauftragten. *Es reicht die Angabe des Kontaktweges z.B. datenschutz@muster-behörde.de*

Verarbeitungstätigkeit

a) Zwecke der Verarbeitung: *Bitte hier eine kurze, prägnante Bezeichnung der Verarbeitungstätigkeit einfügen! (z. B. Name des Forschungsprojekts);*
Erstmeldung/Fortschreibung; Datum der Einführung, Datum der Änderung

b) Angaben zum Prozesseigner/fachlich Verantwortlichen (optional)

c) Rechtsgrundlage der Datenverarbeitung *(z. B.: Die Verarbeitung der Daten erfolgt auf Grundlage einer Einwilligung gem. Art. 6 Abs. 1 lit. a. DSGVO.)*

d) Name des eingesetzten Verfahrens zur Datenerhebung (optional). Soweit eine Software eingesetzt wird, die einen bestimmten Namen/eine bestimmte Bezeichnung trägt oder eine ausführliche Beschreibung des Verfahrens sinnvoll erscheint, können diese Angaben hier erfolgen.

e) Beschreibung der Kategorien betroffener Personen *(wenn eine Kategorienbildung nicht möglich ist, bitte eine möglichst genaue Beschreibung/Bezeichnung der Eigenschaften/Funktionen der betroffenen Personen angeben)*
f) Beschreibung der Daten
g) Empfänger der Daten: *Zugriffsberechtigte (intern, extern, Drittland)*
h) Datenübermittlung: *erfolgt nicht und ist auch nicht geplant, erfolgt in folgender Art und Weise an xxx, Drittland oder internationale Organisation (Rücksprache mit dem Datenschutzbeauftragten halten), Dokumentation der gegebenen Garantien*
i) Fristen für die Löschung *(Hinweis: personenbezogene Daten sind spätestens zum Zeitpunkt des Wegfalls des mit der Speicherung verfolgten Zwecks zwingend zu löschen bzw. vollständig zu anonymisieren, d.h. Löschung des Zuordnungsschlüssels! (vgl. Art. 89 Abs. 2 DSGVO, §§ 45, 50 BDSG). Planen Sie die Daten auf Open-Data-Servern zu speichern, verwenden Sie für pseudonymisierte Daten nur Open-Data-Server (Forschungsdatenzentren), die die Nutzung auf wissenschaftliche Zwecke begrenzen (scientific use). Alternativ zur Speicherung auf einem Open-Data-Server können Sie auch eine kontrollierte Datenfernverarbeitung anbieten. Dabei wird eine von Forschenden auf Basis von Testdatensätzen erstellte Syntax an das Forschungsdatenzentrum übermittelt und ausschließlich durch das Personal vor Ort auf Grundlage der Originaldaten verarbeitet.*

Technische und organisatorische Maßnahmen

Etliche der Punkte können wahrscheinlich nur in Rücksprache mit der IT-Abteilung der Forschungseinrichtung beantwortet bzw. realisiert werden.

a) Die Verarbeitung der Daten wird auf den IT-Systemen der Forschungseinrichtung durchgeführt: *Ja, Nein, teilweise (z. B. nicht zentral administrierte Laptops, PCs, Cloud-Speicher; bitte erläutern)*
b) Pseudonymisierung wird wie folgt eingesetzt: *Pseudonymisierungsregel beschreiben*
c) Verschlüsselung, Passwortschutz wird wie folgt eingesetzt: *Anforderungen Passwort erläutern; Datenverschlüsselung, falls eingesetzt erwähnen (z. B.: BitLocker, FileVault usw.)*
d) Gewährleistung der Vertraulichkeit: *Hier geht es um alles, was Zutritt und Zugang betrifft, Wie wird der Zugang auf Berechtigte begrenzt (z. B.: Passwortschutz, Bildschirmschoner, Verschließen der Büros, Begrenzung der Zugriffsrechte auf die zuständigen Bediensteten; Passwortrichtlinie; automatische Bildschirmsperre; Aktenvernichter; Datenschutztonne)?*
e) Gewährleistung der Integrität: *Wie wird gewährleistet, dass die Daten, die verarbeitet werden, an sich richtig sind? Wie werden Änderungen oder Löschungen gesteuert? Z. B.: Überprüfbarkeit / Nachvollziehbarkeit von Änderungen (Logs, Datenpflege); technische Protokollierung der Eingabe, Änderung und Löschung von Daten; Plausibilitätskontrolle bei Eingabe, Änderung und Löschung; usw.)*
f) Gewährleistung der Verfügbarkeit: *Wie wird, z. B. bei einem Stromausfall die Verfügbarkeit der Daten gewährleistet (z. B. Datensicherungskonzept, bei Servern auch unterbrechungsfreie Stromversorgung u. Ä.)?*
g) Gewährleistung der Belastbarkeit der Systeme: *Werden regelmäßige Checks gemacht, ob die Systeme gegen Unfälle oder Eindringlinge ausreichend gesichert sind?*
h) Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall: *Gibt es Vorgehensweisen zur Wiederherstellung bei einem Zwischenfall, der z. B. alle ihre Daten auf einem Server/PC löscht?*

i) Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen: *Wird auch geprüft, ob die o.g. Maßnahmen effektiv sind? Wenn ja, wie? (z. B. jährliche Überprüfung und Überarbeitung)*

Das Verfahrensverzeichnis kann ergänzt werden durch:

- interne Verhaltensregeln, Dienstvereinbarungen, Arbeitsanweisungen, Standard Operating Procedures (SOP); Risikoanalyse; Datensicherheitskonzept; Wiederanlaufkonzept; Zertifikat / Zertifizierungsstelle

Das Verfahrensverzeichnis wird durch die/den Ersteller sowie die verantwortliche Leitung der Organisationseinheit mit Ort und Datum unterschrieben.