UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Ausfüllhinweise zum Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gemäß Art. 30 DSGVO [1]

Dieses Dokument basiert auf den im Februar 2018 veröffentlichten Hinweisen der Datenschutzkonferenz (DSK). (https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf) Diese wurden an das Muster für Verzeichnisse von Verarbeitungstätigkeiten der Universität Paderborn angepasst und sollen als Ausfüllhilfe dienen.

Änderungshistorie

Was?	Wer?	Wann?
Version 1.0	Klapper/Brennecke	2018
Version 2.0	Klapper/Brennecke	6.6.2019

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Inhalt

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen (Wenn nichts weiter angegeben ist, wird damit die neue seit 25. Mai 2018 geltende Fassung referenziert. Ansonsten wird explizit auf die gleichnamige alte Fassung verwiesen.)
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
ErwGr.	Erwägungsgrund (Der DSGVO vorangestellte Erläuterungen für deren Auslegung)
i. V. m.	in Verbindung mit
lit.	Buchstabe
S.	Satz
VwVfG NRW	Verwaltungsverfahrensgesetz für das Land Nordrhein-Westfalen
z. B.	zum Beispiel

Im Rahmen der Nachweispflichten der EU-Datenschutz-Grundverordnung (DSGVO) muss jeder Verantwortliche und jeder Auftragsverarbeiter ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten erstellen und führen. Die bis Mai 2018 in Nordrhein-Westfalen zu führenden Verfahrensverzeichnisse[2] werden hinfällig und durch die Anforderungen an die neuen Verzeichnisse der Verarbeitungstätigkeiten ersetzt. Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft der Hochschule als Verantwortliche für die Datenverarbeitung dabei, gemäß Art. 5 Abs. 2) nachzuweisen, dass die Vorgaben aus der DSGVO eingehalten werden (Rechenschaftspflicht). Es stellt somit ein wesentliches Element für die Etablierung eines umfassenden Datenschutz- und Informationssicherheits-Managementsystems dar.

1 Zweck des Verzeichnisses

Verantwortliche und Auftragsverarbeiter führen zum Nachweis der Einhaltung der DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.[3]

Dieses Verzeichnis betrifft sämtliche ganz oder teilweise automatisierten Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem[4] gespeichert sind oder gespeichert werden sollen. Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung nach Maßgabe des Art. 30 DSGVO anzufertigen. Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Es ist ein strenger Maßstab anzulegen, so dass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt. Bei einer nur geringen Zweckänderung muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit angepasst werden muss oder ob eine vollständig neue Beschreibung anzufertigen ist. Die Summe der Einzelbeiträge ergibt das Verzeichnis von Verarbeitungstätigkeiten.

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DSGVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist aber ein wichtiger Baustein, um der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht zu genügen. So müssen bspw. auch das Vorhandensein von Einwilligungen[5], die Ordnungsmäßigkeit der gesamten Verarbeitung[6] und das Ergebnis von Datenschutz-Folgenabschätzungen[7] durch entsprechende Dokumentationen nachgewiesen werden.

Um Redundanzen zu vermeiden und den Aufwand für die Erstellung und Führung des Verzeichnisses zu reduzieren, können in die einzelnen Beschreibungen Verweise auf bestehende Dokumente aufgenommen werden. Dies gilt besonders für Dokumente, die im Rahmen des Informationssicherheitsmanagements angelegt wurden, ohne dass sie in das Verzeichnis übernommen werden müssen. So wird bspw. ein hochschulweites Informationssicherheitsrahmenkonzept nur einmal erstellt werden. In verfahrensspezifische Konzepte sind dann nur noch zusätzliche oder abweichende technische und organisatorische Maßnahmen aufzunehmen.

Jeder Verantwortliche und jeder Auftragsverarbeiter ist verpflichtet, mit der Datenschutz-Aufsichtsbehörde[8] zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die einzelnen Verarbeitungsvorgänge bzw. -verfahren anhand dieser Verzeichnisse kontrolliert werden können. Sofern auf bestehende Konzepte verwiesen wird, sollten diese der Datenschutz-Aufsichtsbehörde ebenfalls auf Anforderung

---

[2] Geregelt in § 8 DSG NRW alte Fassung.

[3] Vgl. Art. 30 sowie Erwägungsgrund 82 DSGVO

[4] Ein Dateisystem ist nach Art. 4 Nr. 6 DSGVO „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird".

[5] Vgl. Art. 7 Abs. 1 DSGVO.

[6] Vgl. Art. 24 Abs. 1 DSGVO.

[7] Vgl. Art. 35 Abs. 7 DSGVO.

[8] Zuständige Datenschutz-Aufsichtsbehörde für die öffentlichen Hochschulen in NRW:
Landesbeauftragte für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
Postfach 20 04 44
40102 Düsseldorf
https://www.ldi.nrw.de/metanavi_Kontakt/index.php.

vorgelegt werden. Sind die Konzepte in Gänze nicht vorlegbar, so müssen zumindest die für die Kontrollen relevanten Teile vorgelegt werden.

Die neue Regelung in Art. 30 DSGVO verpflichtet nicht nur jeden Verantwortlichen für die Verarbeitung von personenbezogenen Daten im Sinne von Art. 4 Nr. 7 DSGVO (hierzu zählen auch Hochschulen), sondern nun auch Hochschulen als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO, ein Verzeichnis von Verarbeitungstätigkeiten, welche sie im Auftrag durchführen, zu erstellen und zu führen.

Neben der Umsetzung der Verpflichtung nach Art. 30 DSGVO kann das Verzeichnis als Grundlage zur Erfüllung weiterer datenschutzrechtlicher Pflichten verwendet werden. Aus diesem Grund bietet es sich an, das Verzeichnis auch für folgende Zwecke zu verwenden:

- für eine Festlegung der Verarbeitungszwecke,
- für Zwecke der Rechenschafts- und Dokumentationspflicht,
    - als Nachweis der Rechtmäßigkeit der Verarbeitung,
    - als Nachweis der Datenminimierung,
    - als Nachweis der Richtigkeit und Aktualität der Daten,
- als geeignete Maßnahme zur Erfüllung der Betroffenenrechte,
- zur Schaffung und als Nachweis geeigneter technischer und organisatorischer Maßnahmen,
- zur Prüfung, ob eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO erfolgen muss,
- als Basis für die Aufgabenerfüllung des Datenschutzbeauftragten nach Art. 39 DSGVO.

Dazu wurde das Muster „Verzeichnis von Verarbeitungstätigkeiten“, auf das sich diese Hinweise beziehen, erweitert und zusätzliche Informationen aufgenommen, z. B. Rechtsgrundlage für die Verarbeitung, zugriffsberechtigte Personen(-gruppen) Erfüllung der Informationspflichten und Angaben zur Datenschutzfolgenabschätzung.

2 Vorlage des Verzeichnisses

Der Datenschutz-Aufsichtsbehörde müssen die Verzeichnisse der Verarbeitungstätigkeiten mit den Angaben nach Art. 30 DSGVO auf Anfrage zur Verfügung gestellt werden.[9]

Ziel ist es, dass die Datenschutz-Aufsichtsbehörde die Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrollieren kann. Sofern die Datenschutz-Aufsichtsbehörde ihre Untersuchungen auf bestimmte Verarbeitungstätigkeiten beschränkt, sind nach Maßgabe der Erforderlichkeit nur die dafür relevanten Abschnitte des Verzeichnisses vorzulegen.

Die bisherige Regelung in § 8 DSG NRW alte Fassung, welche ein allgemeines öffentliches Verfahrensverzeichnis mit einem Einsichtsrecht für jedermann sowie eine detaillierte interne Verarbeitungsübersicht beim Datenschutzbeauftragten vorsah, entfällt. An Stelle des öffentlichen Verfahrensverzeichnisses treten die Informationspflichten gegenüber den von der Verarbeitung betroffenen Personen.[10]

3 Form des Verzeichnisses

3.1 Sprache

Das Verzeichnis von Verarbeitungstätigkeiten ist regelmäßig in deutscher Sprache zu führen, § 23 Abs. 1 und 2 VwVfG NRW.

3.2 Schriftform

Die Verzeichnisse sind gemäß Art. 30 Abs. 3 DSGVO schriftlich zu führen. Dies kann auch in einem elektronischen Format erfolgen.

[9] Vgl. Art. 30 Abs. 4 DSGVO und ErwGr. 82.
[10] Vgl. Art. 13 und 14 DSGVO.

Die Datenschutz-Aufsichtsbehörde kann das Format der Vorlage (schriftlich in Papierform oder elektronisch in Textform) eigenständig festlegen und daher auch bei einem im elektronischen Format geführten Verzeichnis den Ausdruck verlangen.[11]

Maßstab sind die Verhältnismäßigkeit und Erforderlichkeit für die jeweils verfolgten aufsichtlichen Zwecke (z. B. nur der erforderliche Teil wird ausgedruckt).

4 Ausfüllhinweise

Im folgenden Kapitel werden zu den einzelnen Abschnitten des Musters „Verzeichnisse von Verarbeitungstätigkeiten“ Informationen und Hilfestellungen zum Ausfüllen bereitgestellt.

Das Verzeichnis muss sämtliche der in Art. 30 Abs. 1 S. 2 lit. a bis g DSGVO abschließend genannten Angaben enthalten. Sie müssen die Verarbeitungstätigkeiten aussagekräftig beschreiben. Zusätzlich sieht das Muster Angaben vor, um die weiteren verarbeitungsspezifischen Dokumentationspflichten aus der DSGVO zu erfüllen und der Rechenschaftspflicht umfassend nachzukommen.

Sollten Sie dem Verzeichnis etwaige Anlagen (Prozessbeschreibungen, Sicherheitskonzepte o. ä.) anfügen, so sind diese im Anlagenverzeichnis am Ende des Dokuments zu verzeichnen.

Angaben im Kopf

Lfd. Nummer	Die Verzeichnisse aller Verarbeitungen an der Universität Paderborn werden an einer zentralen Stelle verwaltet. Die zentrale Stelle vergibt die jeweilige Nummer der Verarbeitungstätigkeit.
Benennung	Tragen Sie an dieser Stelle den Namen für die dokumentierte Verarbeitungstätigkeit ein. Es ist zu empfehlen, den Namen der jeweiligen Verarbeitungstätigkeit von dem Verarbeitungszweck ausgehend festzulegen (z. B. „Personalaktenführung“/„Stammdaten“, „Lohn-, Gehalts- und Bezügeabrechnung“ usw.).

A. Vorblatt

Das Vorblatt. wird lediglich für die Herausgabe an die Aufsichtsbehörde verwendet. Es ist für die hochschulinterne Verwendung des Verzeichnisses nicht erforderlich. Es enthält nur die Angaben zum Verantwortlichen und die Kontaktdaten der/des Datenschutzbeauftragten.

Verantwortlich für die Verarbeitung personenbezogener Daten an der Universität Paderborn ist grundsätzlich die Universität Paderborn als juristische Person.

Die Angaben auf dem Vorblatt sind nicht zu ändern.

Hochschulinterne Kontaktdaten

Die Aufsichtsbehörde wendet sich bei Fragen, Prüfungen etc. über die offiziellen Kontaktangaben bzw. die Datenschutzbeauftragten an den Verantwortlichen.

Innerhalb der Hochschule ist darüber hinaus zur Organisation und Umsetzung des Datenschutzes die Angabe zu den „Betreibern“ einzelner Verarbeitungen erforderlich. Je nach aktueller Frage oder Aufgabe ist es notwendig, dazu einen fachlichen oder technischen Ansprechpartner kontaktieren zu können.

[11] Vgl. § 3a VwVfG NRW.

3. Innerorganisatorische Ansprechpartner

Anzugeben sind zusätzlich zum Bereich / zur Fachabteilung, in dem die Verarbeitung betrieben wird, Namen und Kontaktdaten (Telefonnummer und E-Mail-Adresse) der fachlichen und technischen Ansprechpartner.

4. Datenschutzbeauftragter

Die Angaben ermöglichen den Betreibern sowie Erstellern/Ausfüllern des Verzeichnisses bei Fragen den Datenschutzbeauftragten zu kontaktieren und sind vorausgefüllt.

Änderungshistorie

Um Änderungen der Eintragungen im Verzeichnis nachvollziehen zu können (z. B. wer war wann Verantwortlicher, Datenschutzbeauftragter etc.), soll eine Dokumentation der Änderungen mit einer Speicherfrist von einem Jahr erfolgen. Dies lässt sich auch aus dem Grundsatz der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO herleiten. Hieraus ergibt sich mit Art. 6 Abs. 1 lit. c) DSGVO (Erfüllung einer rechtlichen Pflicht der Hochschule) die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten zu den Änderungen und Revisionen.

B. Angaben zur Verarbeitungstätigkeit

Lfd. Nummer	Vgl. Ausführungen zum Feld „Lfd. Nummer“ im Abschnitt 4.
Benennung	Vgl. Ausführungen zum Feld „Benennung“ im Abschnitt 4.
Datum der Einführung	Geben Sie hier das Datum an, an welchem die Verarbeitungstätigkeit erstmalig eingeführt wurde.
Datum der Änderung	Geben Sie das Datum der Einführung (bei einer neuen Verarbeitungstätigkeit) oder das Datum der letzten Änderung (bei einer bestehenden Verarbeitungstätigkeit) an. Wählen Sie bitte in den Checkboxen in der folgenden Zeile, ob es sich um eine neue Verarbeitungstätigkeit oder die Änderung einer bereits existierenden Verarbeitungstätigkeit handelt.

1. Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen

Rechtsgrundlage: Art. 26, Art. 30 Abs. 1 S. 2 lit. a DSGVO

Dieser Abschnitt ist nur dann auszufüllen, wenn eine gemeinsame Verantwortung nach Art. 26 DSGVO vorliegt. Dies ist nur dann der Fall, wenn die Universität als Verantwortlicher mit einer anderen verantwortlichen Stelle außerhalb der Universität kooperiert und eine gemeinsame Verantwortlichkeit feststellt und vereinbart.

Hier sind keine hochschulinternen Bereiche oder Personen einzutragen.

Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Anzugeben sind die postalische, elektronische und telefonische Erreichbarkeit eines gemeinsam Verantwortlichen.

2. Zweck(e) und Rechtsgrundlage(n) der Verarbeitung

Rechtsgrundlage: Art. 30 Abs. 1 S. 2 lit. b DSGVO sowie
Art. 5 Abs. 1 lit. a i. V. m. Art. 6 Abs. 1 DSGVO

Für jede Verarbeitung sind vor Inbetriebnahme der Verarbeitung die Zwecke festzulegen. Die Zwecke müssen eindeutig und so aussagekräftig sein, dass die Datenschutzbeauftragten und die Datenschutzaufsichtsbehörde

die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung vorläufig einschätzen können. Verarbeitungszwecke sind beispielsweise:

- Personalaktenführung/Stammdaten
- Lohn-, Gehalts- und Bezügeabrechnung
- Arbeitszeiterfassung
- Urlaubsdatei
- Nutzungsprotokollierungen IT/Internet/E-Mail
- Bewerbungsverfahren für Beschäftigte
- Telefondatenerfassung
- Parkplatzverwaltung
- Videoüberwachung an Arbeitsplätzen o. ä.
- Studienplatzbewerbung
- Studierendenverwaltung
- Prüfungsverwaltung
- Beschaffung/Einkauf/Finanzbuchhaltung

Kurze Beschreibung der Verarbeitung	Damit die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung einschätzen kann, ist den einzelnen Verarbeitungszwecken eine kurze Beschreibung der Verarbeitungstätigkeit voranzustellen.

Die Angabe der einzelnen Verarbeitungszwecke erfolgt aufgeschlüsselt nach der jeweiligen Rechtsgrundlage. Die Rechtsgrundlagen sind gemäß ihrer Bedeutung für Hochschulen sortiert.

Rechtsgrundlage: Im öffentlichen Interesse liegende Aufgabe und Ausübung öffentlicher Gewalt **(Art. 6 Abs. 1 lit. e DSGVO)**	Die Verarbeitung personenbezogener Daten aufgrund dieser Rechtsgrundlage ist rechtmäßig, wenn die Verarbeitung zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung verantwortlichen übertragen wurde. Sofern diese Rechtsgrundlage auf den Verarbeitungszweck/die Verarbeitungszwecke zutrifft, so geben Sie den/die Zweck(e) in dieser Zeile an. Nennen Sie zusätzlich die konkretisierende Rechtsgrundlage oder beschreiben Sie die übertragene Aufgabe inklusive einer Begründung ihrer Erforderlichkeit. In der Regel werden die Aufgaben der Hochschulen im Hochschulgesetz (HG NRW) festgelegt sein und ggf. über Ordnungen der Hochschule konkretisiert (bspw. Einschreibungsordnung).
Rechtsgrundlage: Rechtliche Verpflichtung **(Art. 6 Abs. 1 lit. c DSGVO)**	Die Verarbeitung personenbezogener Daten aufgrund dieser Rechtsgrundlage ist rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der die Universität Paderborn unterliegt, erforderlich ist. Sofern diese Rechtsgrundlage auf den Verarbeitungszweck/die Verarbeitungszwecke zutrifft, so geben Sie den/die Zweck(e) in dieser Zeile an. Nennen Sie zusätzlich die zugrundliegende rechtliche Verpflichtung.
Rechtsgrundlage: Einwilligung des Betroffenen **(Art. 6 Abs. 1 lit. a DSGVO)**	Die Verarbeitung personenbezogener Daten aufgrund dieser Rechtsgrundlage ist rechtmäßig, wenn die betroffenen Personen ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten gegeben haben. Sofern diese Rechtsgrundlage auf den Verarbeitungszweck/die Verarbeitungszwecke zutrifft, so geben Sie den/die Zweck(e) in dieser Zeile an. Nehmen Sie die Einwilligungserklärung als Anlage auf oder verweisen Sie auf die Einwilligungserklärung (bspw. Weblink).

Rechtsgrundlage: Vertrag **(Art. 6 Abs. 1 lit. b DSGVO)**	Die Verarbeitung personenbezogener Daten aufgrund dieser Rechtsgrundlage ist rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrages, mit der betroffenen Person erforderlich ist. Sofern diese Rechtsgrundlage auf den Verarbeitungszweck/die Verarbeitungszwecke zutrifft, so geben Sie den/die Zweck(e) in dieser Zeile an. Nennen Sie den geschlossenen Vertrag als Anlage oder verweisen Sie darauf (bspw. Weblink).
Rechtsgrundlage: Wahrung berechtigter Interessen **(Art. 6 Abs. 1 lit. f DSGVO)**	Die Verarbeitung personenbezogener Daten aufgrund dieser Rechtsgrundlage ist rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen der Universität Paderborn oder eines Dritten erforderlich ist. Die Verarbeitung auf der Basis berechtigter Interessen ist für Hochschulen als Behörden in Erfüllung ihrer Aufgaben ausgenommen. Sofern diese Rechtsgrundlage auf den Verarbeitungszweck/die Verarbeitungszwecke zutrifft, so geben Sie den/die Zweck(e) in dieser Zeile an. Begründen Sie zusätzlich das berechtigte Interesse und geben sie ggf. vorhandene Ergebnisse der Prüfung der Verhältnismäßigkeit an.
Rechtsgrundlage: Schutz lebenswichtiger Interessen **(Art. 6 Abs. 1 lit. d DSGVO)**	Die Verarbeitung personenbezogener Daten aufgrund dieser Rechtsgrundlage ist rechtmäßig, wenn die Verarbeitung erforderlich ist um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Sofern diese Rechtsgrundlage auf den Verarbeitungszweck/die Verarbeitungszwecke zutrifft, so geben Sie den/die Zweck(e) in dieser Zeile an. Nennen Sie zusätzlich die lebenswichtigen Interessen, die durch die Verarbeitung geschützt werden.

3. Beschreibung der Kategorien von personenbezogenen Daten

Rechtsgrundlage: Art. 30 Abs. 1 S. 2 lit. c DSGVO

Zu beschreiben sind die Kategorien personenbezogener Daten, d. h. nicht die konkret gespeicherten Daten sondern eine aussagekräftige Beschreibung der Art der Daten und möglichst eine Konkretisierung durch die Aufzählung von Einzeldaten. (Stammdaten allein ist bspw. wenig aussagekräftig, besser Stammdaten der Studierenden (Name, Matrikelnummer, Adresse))

Lfd. Nr.	Vergeben Sie hier laufende Nummern für jede Kategorie personenbezogener Daten. Die laufende Nummer dient dazu, bei komplexen Verarbeitungen den einzelnen Kategorien personenbezogener Daten im Folgenden die Kategorien betroffener Personen, Löschfristen und die Kategorien von Empfängern zuzuordnen.[12]
Kategorien personenbezogener Daten	Nennen Sie hier die Kategorien personenbezogener Daten, die im Rahmen der Verarbeitungstätigkeit gespeichert oder verarbeitet werden. **Beispiel:** Aufgliederung der Kategorie „Beschäftigtendaten“ in die Datenkategorien: • Beschäftigten-Stammdaten mit Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen etc. • Bewerbungen mit Kontaktdaten, Qualifikationsdaten, Tätigkeiten

[12] Vgl. Art. 30 Abs. 1 S. 2 lit. d bis g DSGVO.

	etc. • Arbeitszeugnisse mit Adressdaten, Leistungsdaten, Beurteilungsdaten etc. • Abmahnungen mit Adressdaten, Arbeitsverhalten, Leistungsdaten etc. • Betriebsarztuntersuchungen mit Adressdaten etc. • Stundenplan als Einsatzplan für Lehrkräfte **Beispiel:** Aufgliederung der Kategorie „Studierendendaten“ in die Datenkategorien: • Stammdaten mit Adressdaten, Geburtsdatum • Hochschulzugangsberechtigung • Hochschulvergangenheit • Anträge • Gebühren und Zahlungen **Beispiel:** Aufgliederung der Kategorie „Prüfungsdaten“ in die Datenkategorien: • Gewählte Studiengänge mit Fächern und Schwerpunkten • Belegte Kurse und Veranstaltungen, ggf. mit Noten • Sperren an Leistungen • Prüfer
Werden besondere Kategorien personenbezogener Daten (Art. 9) verarbeitet?	Aufgrund Ihres besonderen Schutzbedarfes ist die Verarbeitung besonderer Kategorien personenbezogener Daten i. S. d. Art. 9 Abs. 1 DSGVO gesondert zu beschreiben. Sobald besondere Kategorien personenbezogener Daten im Rahmen der Verarbeitungstätigkeit verarbeitet werden, so geben Sie dies hier an. Unter die besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO fallen: • Rassische und ethnische Herkunft • Politische Meinungen • Religiöse oder weltanschauliche Überzeugungen • Gewerkschaftszugehörigkeit • Genetische Daten • Biometrische Daten • Gesundheitsdaten • Sexualleben sowie sexuelle Orientierung
Lfd. Nr.	S. o. Ausführungen zum Feld „Lfd. Nr.“
Besondere Kategorien personenbezogener Daten	Nennen Sie hier die besonderen Kategorien personenbezogener Daten, die im Rahmen der Verarbeitungstätigkeit gespeichert oder verarbeitet werden.

4. Beschreibung der Kategorien betroffener Personen

Rechtsgrundlage: Art. 30 Abs. 1 S. 2 lit. c DSGVO

Zu beschreiben sind die Kategorien betroffener Personen. Hierzu sind Personengruppen aus dem Hochschulkontext vorgegeben, die bei Bedarf ergänzt werden müssen.

Lfd. Nr. aus 3	Um eine Zuordnung der Kategorien personenbezogener Daten zu den

	Kategorien betroffener Personen zu ermöglichen, ist es notwendig, die einzelnen Daten-Kategorien nach den Kategorien betroffener Personen aufzuschlüsseln. Geben Sie aus diesem Grund die in 3. vergebenen laufenden Nummern der Kategorien personenbezogener Daten für die einzelnen Personen-Kategorien an.
Kategorien betroffener Personen	Wählen Sie in diesem Bereich die Kategorien der von der Verarbeitungstätigkeit betroffenen Personen-Kategorien aus. Sollte die von Ihrer Verarbeitung betroffene Personen-Kategorie nicht Bestandteil der Liste sein, so ergänzen Sie diese bitte.

5. Fristen für die Löschung der verschiedenen Datenkategorien

Rechtsgrundlage: Art. 30 Abs. 1 S. 2 lit. f DSGVO

Löschkonzept und Löschregeln	Wählen Sie hier aus, ob das Löschkonzept in einem eigenen Dokument beschrieben wird oder nennen Sie die einzelnen Löschregeln im darauffolgenden Abschnitt „Löschregeln“ (s. u.). Falls Sie über ein separates Löschkonzept verfügen, so nehmen Sie dieses als Anlage auf.
Löschregeln für die Datenkategorien	Geben Sie bitte die einzelnen Löschregeln für die im Abschnitt 3 erhobenen Datenkategorien an. **Lfd. Nr. aus 3:** Geben Sie hier die in 3. vergebenen laufenden Nummern der Kategorien personenbezogener Daten an. Eine Löschregel besteht immer aus einem Startzeitpunkt (bspw. das Erhebungsdatum, das Einschreibungsdatum, das Ende eines Semesters, ein Vertragsende, das Ende eines Forschungsprojekts) sowie einer Löschfrist, die den Zeitraum zwischen Startzeitpunkt und Löschung festlegt. Die Fristen ergeben sich bspw. aus gesetzlich geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Finanz- und Personaldaten, von der Hochschule geregelten Aufbewahrungs- und Löschfristen für Prüfungsunterlagen. **Startzeitpunkt des Fristablaufs/Auslöser der Frist:** Beschreiben Sie hier ab wann die Frist zur Löschung der genannten Datenkategorie beginnt. **Löschfrist/Zeitraum bis zur Löschung:** Nennen Sie in dieser Spalte den Zeitraum bis zur Löschung.

Sofern Sie keine konkreten Löschregeln angeben können, so geben Sie bitte entsprechende **Kriterien für die Festlegung der Speicherdauer** an. Ein allgemeiner Verweis auf Aufbewahrungspflichten genügt nicht, es sind präzise Angaben erforderlich.

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

Rechtsgrundlage: Art. 30 Abs. 1 S. 2 lit. d DSGVO

Lfd. Nr. aus 3	Um eine Zuordnung der Kategorien personenbezogener Daten zu den betroffenen Personen zu ermöglichen, ist es notwendig, die einzelnen Daten-Kategorien nach den Kategorien betroffener Personen aufzuschlüsseln. Geben Sie aus diesem Grund die in 3. vergebenen laufenden Num-

	mern der Kategorien personenbezogener Daten für die einzelnen Personen-Kategorien an.
Intern (Zugriffsberichte)	Kreuzen Sie dieses Feld an, wenn die Daten weiteren internen Empfängern in der Hochschule offengelegt werden. Geben Sie zusätzlich die Abteilung/en an, denen gegenüber die Daten offengelegt werden.
Extern	Kreuzen Sie dieses Feld an, wenn sich der Empfänger außerhalb der Rechtsperson Universität befindet.
Drittland	Kreuzen Sie dieses Feld an, wenn die Daten gegenüber einem Empfänger in einem Drittstaat oder einer internationalen Organisation offengelegt werden. Ergänzen Sie weitere Informationen zur Übermittlung unter Punkt 7 des Verzeichnisses.

7. Ggf. Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

Rechtsgrundlage: Art. 30 Abs. 1 S. 2 lit. e DSGVO

Empfänger in Drittländern und internationale Organisationen sind keine Kategorien von Empfängern und daher konkret zu benennen. Handelt es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung, sind angemessene Garantien im Verzeichnis zu dokumentieren. Erfolgt die Datenübermittlung zu Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Rechte ausüben, entfällt die Pflicht, geeignete Garantien zu dokumentieren.

Sie sollten vor der Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation in jedem Falle den Datenschutzbeauftragten beteiligen.

Datenübermittlung an ein Drittland oder internationale Organisation	Geben Sie hier an, ob die im Rahmen der Verarbeitung erhobenen oder verarbeiteten Daten an einen Drittstaat außerhalb der EU oder eine internationale Organisation übermittelt werden. Falls eine Datenübermittlung an ein Drittland oder eine internationale Organisation stattfindet, so ist die Übermittlung kurz zu beschreiben.
Nennung der konkreten Datenempfänger	Wählen Sie aus, ob es sich bei den konkreten Datenempfängern um einen Empfänger in einem Drittland oder um eine internationale Organisation handelt. Geben Sie zudem
Dokumentation geeigneter Garantien	Geben Sie hier an, welche Garantien es für die Datenübermittlung und Verarbeitung gibt. Möglich sind: • Übertragung in einen anerkannten Drittstaat mit Angemessenheitsbeschluss der EU-Kommission • Verwendung der EU-Standarddatenschutzklauseln • Genehmigung des Vertrags durch die Aufsichtsbehörden • Sicherstellung eines ausreichenden Datenschutzniveaus durch bindende Verhaltensregeln • Sicherung eines ausreichenden Datenschutzniveaus durch einen Zertifizierungsmechanismus sowie daraus resultierender Selbstverpflichtung • Herstellung des ausreichenden Datenschutzniveaus durch sonstige Maßnahmen. Sollte dies der Fall sein, so beschreiben Sie die sonstigen Maßnahmen bitte nachfolgend.

	Wenn keine von den oben genannten Garantien zur Sicherstellung des Datenschutzniveaus zutrifft, geben Sie den geltenden Ausnahmetatbestand des Art. 49 DSGVO an.

C. Weitere Angaben

1. Welche Personengruppen haben Zugriff auf welche der erhobenen personenbezogenen Datenkategorien?

Rechtsgrundlage: Art. 5 Abs. 1lit. b, c DSGVO

Berechtigungskonzept oder Zugriffsberechtigungen	Wählen Sie hier aus, ob das Berechtigungskonzept in einem eigenen Dokument beschrieben wird oder nennen Sie die einzelnen Zugriffsberechtigungen im darauffolgenden Abschnitt „Zugriffsberechtigte Personengruppen“ (s. u.). Falls Sie über ein separates Berechtigungskonzept verfügen, so nehmen Sie dies als Anlage auf.
Lfd. Nr. aus B.3	Um die Zuordnung der einzelnen Kategorien personenbezogener Daten zu den zugriffsberechtigten Personengruppen herzustellen, sind in dieser Spalte die im Abschnitt B.3 definierten laufenden Nummern für die verarbeiten Kategorien personenbezogener Daten anzugeben.
Zugriffsberechtigte Personengruppen	Beschreiben Sie hier die zugriffsberechtigten Personengruppen für jede Datenkategorie. Es reicht aus, die Zugriffsberechtigten über eine Rollen- oder Funktionsbeschreibung eindeutig bestimmbar zu beschreiben, ohne sie namentlich zu nennen.
Umfang	Wählen Sie hier den Umfang der Zugriffsberechtigung aus.

2. Transparenz/Informationspflichten

Rechtsgrundlage: Art. 5 Abs. 1 lit. a i. V. m. Art. 12 ff. DSGVO

Im Rahmen der Transparenz und Informationspflichten ist die Art und Weise der Information der Betroffenen über die Erhebung zu erfassen. Wählen Sie an dieser Stelle aus, ob

- Die Betroffenen mittels eines Informationsblatts über die Erhebung informiert werden (wenn dem so ist, fügen Sie es bitte dem Dokument an),
- Die Betroffenen mittels einer Online-Datenschutzerklärung über die Erhebung informiert werden (wenn dem so ist, geben Sie den Link zur Datenschutzerklärung bitte an) oder
- Die Betroffenen auf anderem Wege über die Datenerhebung informiert werden. Sollte dies der Fall sein, so beschreiben Sie bitte zusätzlich die Art und Weise der Information der Betroffenen.

3. Auftragsverarbeitung

Rechtsgrundlage: Art. 28 DSGVO

Angaben zum Auftragsverarbeiter	Geben Sie hier die Kontaktdaten des Auftragsverarbeiters an.

4. Schwellwertanalyse

Rechtsgrundlage: Art. 35 Abs. 1 DSGVO

Die DSGVO verlangt die Durchführung einer Datenschutzfolgenabschätzung (DSFA), wenn die Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen hat. Damit die Datenschutzfolgenabschätzung nicht für jede Verarbeitung komplett durchgeführt werden muss, soll im Rahmen einer Schwellwertanalyse das Risiko der Verarbeitung für die betroffenen Personen abgeschätzt werden.

Dazu wird gemäß der Handreichung zur Datenschutzfolgenabschätzung eine Prüfung in Form der Schwellwertanalyse durchgeführt und das festgestellte Risiko einer Stufe zugeordnet.

Seitens der Informationssicherheit werden Datenverarbeitungen ebenfalls einer Prüfung unterzogen, deren erster Schritt eine so genannte Schutzbedarfsfeststellung ist, die ebenfalls eine Risikobewertung in drei Stufen liefert.

Normales Risiko für die Betroffenen
Hohes Risiko für die Betroffenen
Sehr Hohes Risiko für die Betroffenen

Das festgestellte Risiko ist zu dokumentieren.

Liefern die datenschutzrechtliche Schwellwertanalyse und die sicherheitstechnische Schutzbedarfsfeststellung unterschiedliche Bewertungen, so ist das höhere Risiko einzutragen. Für die Risikoanalyse sollten Datenschutz-Koordinatoren, Datenschutzbeauftragte und Informationssicherheitsbeauftragte hinzugezogen werden.

5. Datenschutzfolgenabschätzung

Rechtsgrundlage: Art. 35 DSGVO

Besteht voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, so muss eine Datenschutzfolgenabschätzung durchgeführt werden. Die Feststellung sollte durch eine Schwellwertanalyse erfolgen (s.o.). Ergibt die Schwellwertanalyse ein normales Risiko, so ist die weitere Datenschutzfolgenabschätzung nicht erforderlich.

Ansonsten muss eine Datenschutzfolgenabschätzung durchgeführt und das Ergebnis dokumentiert werden. Dabei ist der Rat der Datenschutzbeauftragten einzuholen. Diese sollten dazu frühzeitig beteiligt werden.

Im Rahmen der Datenschutzfolgenabschätzung werden die Auswirkungen der vorgesehenen Verarbeitungsvorgänge auf den Schutz personenbezogener Daten geprüft und bewertet. Dazu ist eine systematische Dokumentation der Verarbeitung erforderlich, die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung zu beurteilen und das Risiko für die Betroffenen differenziert zu prüfen. In Abhängigkeit des Risikos sind die für die Verarbeitung getroffene und geplante technische und organisatorische Maßnahmen zu bewerten und ggf. so anzupassen, dass die Risiken der Verarbeitung hinreichend bewältigt werden. Hierfür ist im Rahmen der Datenschutzfolgenabschätzung ein Nachweis zu erbringen.

Das abschließende Ergebnis wird in der Tabelle dokumentiert. Die im Rahmen der Datenschutzfolgenabschätzung erstellte Dokumentation sollte als Anhang aufgenommen werden.

Können die Risiken der Verarbeitung nicht durch geeignete Maßnahmen eingedämmt werden, so ist die Aufsichtsbehörde zu konsultieren. Das Ergebnis der Konsultation muss dokumentiert werden.

D. Technische und organisatorische Maßnahmen (TOM)

Rechtsgrundlage: Art. 30 Abs. 1 lit. f, Art. 32 DSGVO

Trotz der Formulierung „wenn möglich“ in der DSGVO stellt die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO hier den Regelfall dar, ist also in jedem Fall zu erstellen.

Art. 5 Abs. 2 DSGVO verpflichtet den Verantwortlichen insbesondere auch zur Dokumentation der technischen und organisatorischen Maßnahmen (Art. 5 Abs. 1 lit. f DSGVO). Zudem muss der Verantwortliche die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen (Art. 32 Abs. 1 lit. d DSGVO). Beide Forderungen kann der Verantwortliche nur erfüllen, wenn die technischen und organisatorischen Maßnahmen vollständig beschrieben sind (etwa in einem Sicherheitskonzept).

Eine Verarbeitung darf erst erfolgen, wenn der Verantwortliche seiner Pflicht nach Art. 24 DSGVO nachgekommen ist. Darunter fallen neben den Verpflichtungen nach Art. 25 DSGVO (Privacy by design/Privacy by default) auch diejenigen nach Art. 32 DSGVO (Sicherheit der Verarbeitung) zur Bestimmung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das betrifft primär Fragen der Sicherheit der Verarbeitung, schließt somit aber auch Maßnahmen zur Gewährleistung von Betroffenenrechten ein. In das Verzeichnis ist eine allgemeine, einfach nachvollziehbare Beschreibung der für diesen Zweck getroffenen Maßnahmen aufzunehmen. Die Beschreibung der jeweiligen Maßnahme ist konkret auf die Kategorie betroffener Personen bzw. personenbezogener Daten im Sinne des Art. 30 Abs. 1 S. 2 lit. c DSGVO zu beziehen, soweit eine entsprechende Differenzierung in ihrer Anwendung erfolgt.

Eine Verletzung der Sicherheit der Datenverarbeitung ist immer eine Verletzung des Schutzes personenbezogener Daten i. S. v. Art. 4 Nr. 12 DSGVO, sofern personenbezogene Daten verarbeitet werden.

Nach Art. 32 Abs. 1 DSGVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit

und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Maßnahmen zu treffen, um insbesondere Folgendes sicherzustellen:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Dazu gibt es einen Maßnahmenkatalog in dem den einzelnen Bereichen typische, bewährte technische und organisatorische Maßnahmen zugeordnet werden. Die Auflistung ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein. Auch ist die Zuordnung einzelner Maßnahmen zu einem bestimmten Maßnahmenbereich nicht in jedem Fall eindeutig.

Alternativ können andere Dokumentationsformen genutzt werden. Dazu gibt es unterschiedliche Vorlagen. Wurde für eine Verarbeitung bereits ein Sicherheitskonzept erstellt, so kann auf dieses verwiesen werden. Ebenso reicht es aus auf die Ergebnisse eines Audits zu verweisen, wenn bspw. eine informationssicherheitstechnische Prüfung und Zertifizierung erfolgt ist. Zu beachte ist in jedem Fall der Scope der Zertifizierung. Wenn bspw. ein Zertifikat für eine Serverinfrastruktur vorliegt, so sind die anderen Komponenten der Verarbeitung (Anwendung, Clients, …) dennoch zusätzlich zu dokumentieren.

Für die Bestimmung der zu treffenden Maßnahmen wird auf das Standard-Datenschutzmodell, die Leitlinien und Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Artikel-29-Arbeitsgruppe sowie auf die bestehenden nationalen und internationalen Standards (z. B. BSI-Grundschutz, ISO-Standards) verwiesen.