# **Datenschutz-Steckbrief**

# Template zur Dokumentation von Verarbeitungstätigkeiten als Grundlage für eine datenschutzrechtliche Bewertung

# Team Datenschutz der TU Berlin (Stand: März 2022)

Als Antragsteller\*in unterstützen Sie uns bei der datenschutzrechtlichen Bewertung, indem Sie folgende Details zur beantragten Verarbeitungstätigkeit zusammenstellen.

Das Dokument besteht aus zwei Teilen:

1. Verpflichtende Informationen für das Verzeichnis von Verarbeitungstätigkeiten entsprechend Art. 30 DSGVO
2. Weitere Informationen zur datenschutzrechtlichen Einschätzung, die wichtige Details eines Datenschutzkonzepts widerspiegeln

Die Informationen im ersten Teil sind durch den/die Verantwortliche\*n im Verzeichnis von Verarbeitungstätigkeiten zu erfassen, so dass dieses Dokument auch dafür dienen kann.

Im zweiten Teil können Sie einzelne Punkte auslassen, sofern sie aus Ihrer Sicht nicht für die Bewertung erforderlich sind. Falls weitere Aspekte für die Einschätzung relevant sind, bitten wir Sie diese zu ergänzen.

### Hinweise:

* Zum besseren Verständnis geben wir grau hinterlegte Hinweise direkt bei den einzelnen Punkten, zur besseren Lesbarkeit können Sie diese gern bei der Bearbeitung löschen. Die Datenkategorien werden in einer Tabelle im Querformat beschrieben, die dafür eingefügten Abschnittsumbrüche sollten erhalten bleiben.
* Verweisen Sie bei den einzelnen Punkten auf weitere Dokumente, sofern diese zur Einschätzung förderlich sind. Insbesondere falls die Beschreibung umfänglich ist bzw. bereits an anderer Stelle dokumentiert wurde.
* Bei externen Dienstleistern bitte alle Dokumente beifügen (Vertragsentwurf (AVV), DPA, TOMs etc.). Hierbei ist zumeist eine aufwändige Prüfung erforderlich.
* Sofern im Rahmen von Projekten Softwareeinsatz oder -entwicklung vorgesehen sind, bitte die vorhandenen Informationen mit aufnehmen/beifügen, z.B. Projektbeschreibung oder Fachkonzept.
* Im Falle von Kooperationen mit Dritten bitte darlegen, wie die Aufgabenaufteilung und Verantwortlichkeiten geregelt werden, Stichwort Gemeinsame Verantwortung/Joint Control i.S.v. Art. 26 DSGVO.
* Sie können anschließend einige der in diesem Dokument von Ihnen zusammengestellten Informationen in die Datenschutzhinweise für Nutzer\*innen aufnehmen.

# Teil 1 Verpflichtende Informationen für das Verzeichnis von Verarbeitungstätigkeiten entsprechend Art. 30 DSGVO

## ­Datum

*Geben Sie das Datum der Einreichung an.*

## Neuantrag / Änderungsanzeige

*Geben Sie hier an, ob es sich um einen Neuantrag oder um eine Änderung / Nachmeldung zu einer Verarbeitungstätigkeit handelt.*

## Voraussichtlicher zeitlicher Umfang (Bereitstellungsdauer)

*Wann soll die Verarbeitungstätigkeit aufgenommen werden und ob sie befristet betrieben werden soll?*

## Name des Dienstes/der Software

*Geben Sie die Bezeichnung an, unter der die Verarbeitung an der TU Berlin geführt wird und, sofern ein Softwareprodukt zum Einsatz kommt, auch dessen Namen.*

## Art der Verarbeitungstätigkeit

*Geben Sie an, wofür die Verarbeitung erfolgt, beispielsweise Personalaktenverwaltung*

## Verantwortliche\*r für den Betrieb

*Verantwortliche\*r ist in der Regel die Leitung des Bereichs/der Einrichtung, es kann zusätzlich ein\*e Vertreter\*in/Ansprechpartner\*in angegeben werden. Geben Sie jeweils die Kontaktdaten an.*

## Zwecke der Verarbeitung

*Beschreiben Sie kurz, wozu die Verarbeitung dient und welche Ziele damit verfolgt werden.*

## Rechtsgrundlage

*Geben Sie an, auf welcher Basis die personenbezogenen Daten verarbeitet werden. Rechtsgrundlagen für die Verarbeitung personenbezogener Daten können sich aus den unterschiedlichsten Regelwerken ergeben, wie beispielsweise aus dem Berliner Hochschulgesetz (BerlHG), aus der Studierendendatenverordnung (StudDatVO), aus Satzungen der TU Berlin, aus dem Landesbeamtengesetz, Tarifverträgen oder Dienstvereinbarungen.*

*Die Rechtmäßigkeit bestimmt sich nach Art. 6 Abs.1 DSGVO[[1]](#footnote-1), geben Sie bitte an welche Punkte in Frage kommen (ggf. nach Nutzergruppen differenziert):*

## Tabellarische Informationen zu den verarbeiteten Datenkategorien „Datenkategorien-Tabelle“

*Listen Sie in der Tabelle alle Kategorien personenbezogener Daten auf, die verarbeitet werden. In dieser Tabelle werden alle wesentlichen Informationen zu den verarbeiteten personenbezogenen Daten erfasst.*

*Hinweise zu den einzelnen Spalten sind auf der Folgeseite zu finden.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Datenkategorien | Betroffene Personen­gruppen | Datenherkunft | TU-interne Empfänger | TU-externe Empfänger | Transfer in Drittland? | Aufbewahrungsfrist (Wann werden die Daten gelöscht) |
| *Bsp.* | *Nutzerkontoinformationen (Account, Name, E-Mail und Status)* | *Studierende, Beschäftigte* | *Übernahme aus IDM der TU* | *ZUV/Buchhaltung*  *Kursleiter\*innen* | *keine* | *nein* | *Bis zum Ende des Folgesemesters (wegen mögl. Nachfragen)* |
| *Bsp.* | *Bankdaten (Name, IBAN, BIC)* | *Studierende, Beschäftigte* | *Selbsteingabe* | *ZUV/Buchhaltung* | *Finanzinstitut* | *nein* | *1 Monat nach Ausführung* |
| 1. |  |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |  |
| 4. |  |  |  |  |  |  |  |
| 5. |  |  |  |  |  |  |  |

## Hinweise zur Datenkategorien-Tabelle

Fassen Sie diejenigen personenbezogenen Daten in Datenkategorien in einer Zeile zusammen, die inhaltlich zueinander gehören und im Verarbeitungskontext einheitlich verarbeitet werden.

Zur Bedeutung der einzelnen Spalten:

* **Nr.**  
  die laufende Nummer wird ggf. für Verweise weiter unten benötigt.
* **Datenkategorien der zu verarbeitenden personenbezogenen Daten:**Geben Sie bitte alle Datenkategorien von personenbezogenen Daten an, die verarbeitet werden.

Datenkategorien umfassen dabei inhaltlich und im Rahmen der Verarbeitung zusammengehörende Datenfelder, d.h. sofern diese übereinstimmende Einträge in der Tabelle haben bzgl. der betroffenen Personengruppen, Datenherkunft, TU-internen und externen Empfängern, Transfer in Drittland und Aufbewahrungsfrist.

Diese sollen jeweils in einer Zeile zusammengefasst werden, beispielsweise

* + **Kontaktinformationen** (Name, Adresse, E-Mail-Adresse, Telefonnummer)
  + **Nutzerkontoinformationen** (Account, Name, E-Mail-Adresse, Status)
  + **Bankdaten** (Name, IBAN, BIC)
  + **Verbindungsdaten** (IP-Adresse und Browserinformationen)
  + **Kommunikationsinhalte** (Text, Bilder, Audio/Video)
* **Betroffene Personengruppen**   
  Geben Sie alle Personengruppen an, deren Daten verarbeitet werden, bspw. Studierende, Beschäftigte oder Interessenten
* **Datenherkunft**  
  Woher stammen die Daten, wurden sie aus einer anderen Quelle übernommen oder hat die\*der Betroffene sie selbst eingegeben?
* **Empfänger (Weitergabe von Daten)**  
  Geben Sie alle Empfänger\*innen von Datenübermittlungen (einschl. Schnittstellen) an, d.h. an wen werden personenbezogene Daten übertragen.   
  Benennen Sie
  + TU-interne Empfänger, d.h. organisatorische Einrichtungen innerhalb der TUB (z.B. ZUV/Buchhaltung) sowie
  + TU-externe Empfänger, d.h. Dritte außerhalb der TUB wie Finanzamt, Drittmittelgeber oder Sozialversicherungen.
* **Übermittlung in Drittländer**   
  Geben Sie an, ob Daten außerhalb der EU/des EWR verarbeitet werden. Sofern dieses bejaht wird, sind weiter unten zusätzliche Garantien zu benennen (unter „Übermittlung in Drittländer“).
* **Aufbewahrungsfrist / Löschkonzept**

Wie lange werden die o.g. Kategorien personenbezogener Daten gespeichert? Eine Frist ist in jedem Fall anzugeben und diese zu begründen.

Die Löschfristen ergeben sich in der Regel aus rechtlichen Vorgaben (z.B. Aufbewahrungsfristen), die Sie bitte angeben. Andernfalls lässt sich ggf. aus dem Zweck der Verarbeitung die Aufbewahrungsfrist ableiten.  
In letzten Fall ist eine nachvollziehbare Begründung für die gewählte Frist erforderlich (z.B. 1 Monat bei Anfragen über Kontaktformulare für Rückfragen).  
Im 2. Teil, Abschnitt „Löschkonzept (einschl. Übergabe an das Universitätsarchiv)“, können die Details näher ausgeführt werden.

# Fortsetzung Teil 1

## Übermittlung in Drittländer

*Sofern personenbezogene Daten außerhalb der EU/des EWR verarbeitet werden, geben Sie bitte an, welche Datenkategorien zu welchen Zwecken weitergegeben werden, bspw.*

* + *Verarbeitung von Metadaten (z.B. bei Videokonferenzanbietern)*
  + *Telemetriedaten oder Absturz- bzw. Fehlermeldungen*
  + *Einbindung von weiteren Diensten/Dienstleistern bei Cloud-Produkten (bitte mit Zweck dokumentieren, ggf. den Beschreibungen des Anbieters entnehmen bzw. diese beifügen)*

*Geben Sie an, auf welcher rechtlichen/vertraglichen Basis die Übermittlung erfolgt (z.B. Standardvertragsklauseln) und welche zusätzlichen Schutzmaßnahmen vereinbart wurden, sog. „supplementary measures“.*

## Werden besondere Kategorien von personenbezogenen Daten verarbeitet?

*Geben Sie bitte an, ob und welche „Besondere Kategorien von personenbezogenen Daten“ nach Art. 9 DSGVO verarbeitet werden (rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschafts­zugehörig­keit, genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben und zur sexuellen Orientierung)*

## Beteiligte Dritte (Dienstleister oder Kooperationspartner)

*Sofern Dienstleister mittels Auftragsverarbeitungsvertrag (AVV) beauftragt werden sollen oder die Verarbeitung mit Dritten in gemeinsamer Verantwortung (Joint Control) umgesetzt wird, geben Sie diese bitte an und ebenso wie die Aufgabenübertragung bzw. -aufteilung erfolgt.   
Fügen Sie die entsprechenden Verträge und Vereinbarungen als Dokument mit bei.*

## Zugriffsberechtigte

*Wer kann die personenbezogenen Daten einsehen, wer kann sie verarbeiten? Differenzieren Sie ggf. entsprechend der obigen Datenkategorien.*

*Geben Sie bitte an, wie Berechtigungen erteilt und verwaltet werden.*

*Beschreiben Sie das Rechte- und Rollenkonzept, verweisen Sie ggf. auf ein separates Dokument.*

## Technische und organisatorische Maßnahmen (TOMs)

*Erläutern Sie die umgesetzten technischen und organisatorischen Maßnahmen, verweisen Sie ggf. auf ein separates Dokument.*

*Die TOMs umfassen: Wie ist der Zutritt zu den Servern/Systemen und der Zugriff darauf und auf die dort verarbeiteten Daten geregelt, welche Sicherungsmaßnahmen (z.B. Verschlüsselung) und welche Backup-Prozesse sind umgesetzt, etc..*

## Datenschutzfolgenabschätzung (DSFA) ist erforderlich?

*Prüfen Sie, ob eine DSFA erarbeitet werden muss. Das Team Datenschutz berät Sie dabei.*

*Besteht ein hohes Risiko für die Betroffenen? Begründen Sie Ihre Einschätzung bspw. mit einer Risikobewertung.*

*Prüfen Sie außerdem, ob es sich um eine Verarbeitungstätigkeit handelt, für die gemäß der aktuellen Positivliste der Berliner Aufsichtsbehörde eine DSFA erforderlich ist? Siehe*[*https://www.datenschutz-berlin.de/wirtschaft-und-verwaltung/datenschutz-folgenabschaetzung*](https://www.datenschutz-berlin.de/wirtschaft-und-verwaltung/datenschutz-folgenabschaetzung) *(Stand Januar 2021 ist die Liste von 10/2018 aktuell).*

*Ende Teil 1*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Teil 2 Weitere Informationen zur datenschutzrechtlichen Einschätzung

## Zielgruppe

*Geben Sie an, an welchen Personenkreis von Nutzer\*innen sich das Angebot richtet, z.B. TU-Externe, Beschäftigte oder Studierende.*

## Nutzungsszenarien

*Geben Sie einige beispielhafte Anwendungsfälle an, auch in welchem Kontext die Software zum Einsatz kommen soll, z.B. Lehre, Forschung oder Verwaltung.*

## Funktionalität

*Geben Sie eine Kurzbeschreibung des Funktionsumfangs der Software an, verweisen Sie ggf. auf ein weiteres Dokument.*

## Anforderungen an Geräte und Betriebssysteme

*Geben Sie bitte an, welche Voraussetzungen für die Software bei den Anwender\*innen gefordert werden, z.B. Installation einer App oder Nutzung im Browser. Sofern nur bestimmte Betriebssysteme und/oder Browser-Versionen unterstützt werden, dieses bitte auch angeben.*

## Technische Umsetzung

*Geben Sie die Rahmenbedingungen an, z.B. ob die Software im TU-eigenen Rechenzentrum oder bei Drittanbietern betrieben wird und welcher Bereich den ordnungsgemäßen Betrieb gewährleistet.*

*Ggf. ist es sinnvoll, technische Details anzugeben, z.B. Virtualisierung/VM, Betriebssystem, Plattform und eingesetzte Komponenten.*

*Geben Sie an, welche Installations- und Konfigurationseinstellungen möglich sind und ausgewählt werden sollen, um die Software datenschutzfreundlich zu betreiben.*

## Darstellung der Datenflüsse

*Beschreiben Sie insbesondere bei Nutzung von TU-externen Diensten/Cloud-Produkten, welche Daten wohin übertragen und verarbeitet werden. Fügen Sie ggf. Diagramme oder Beschreibungen des Anbieters bei bzw. verweisen Sie ggf. auf ein weiteres Dokument.*

## Schnittstellen

*Dokumentieren Sie, wie die in der Datenkategorien-Tabelle angegebene Weitergabe von Daten an TU-interne Empfänger sowie externe Stellen umgesetzt werden soll.  
Stellen Sie dabei auch dar, wie eine Integration in die IT-Systemlandschaft erfolgen soll, d.h. welche Schnittstellen zu anderen Systemen der TU (IDM/SSO, ISIS, SAP, etc.) implementiert sind oder werden.*

## Löschkonzept (einschl. Übergabe an das Universitätsarchiv)

*Wie wird die datenschutzgerechte Löschung oder Anonymisierung der personenbezogenen Daten nach Ablauf o.g. Aufbewahrungsfristen umgesetzt? Sofern je Datenkategorien unterschiedlich verfahren werden sollte, dieses bitte differenziert darstellen? Verweisen Sie ggf. auf ein weiteres Dokument.*

*Prüfen und dokumentieren Sie außerdem, ob für die Daten eine Notwendigkeit/Anbietepflicht zur Archivierung/Übergabe an das Universitätsarchiv besteht und wie dieser Genüge getan werden soll.*

## Welche Schritte wurden bisher unternommen?

*Wurde das Softwareprodukt –beispielsweise zu Testzwecken– bereits genutzt? Gibt es eine Software, die ersetzt werden soll? Gab es bereits Kommunikation mit dem Anbieter?*

## Sonstiges

*Alles, was die datenschutzrechtliche Beurteilung erleichtert, z.B. ob es Erfahrungen/Einschätzungen anderer Hochschulen oder Forschungseinrichtungen gibt, ggf. sogar eine datenschutzrechtliche Bewertung?*

*Ende Teil 2*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Art. 6 Abs.1 DSGVO, <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679#d1e1906-1-1> :

   (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

   1. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
   2. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
   3. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
   4. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
   5. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
   6. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

   … Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. [↑](#footnote-ref-1)