Team Datenschutz | K 3 – DS
TU Berlin |Straße des 17. Juni 135 | 10623 Berlin

Team Datenschutz

Annette Hiller
+49 30 314-**21784**
Raum H 1038

Alexander Hoffmeier
+49 30 314-**29595**
Raum H 1042

Dr. Mattis Neiling
+49 30 314-**28973**
Raum H 1042

info@datenschutz.tu-berlin.de

Fax +49 30 314-28033

Unser Zeichen:
K3 - DS

Berlin, 9. Januar 2023

Pilotprojekt: Verzeichnis der Verarbeitungstätigkeiten entsprechend Art. 30 Datenschutz-Grundverordnung (DSGVO)

Liebe Kolleg*innen,

wir informieren Sie darüber, wie das Team Datenschutz die Einrichtungen der TU Berlin dabei unterstützen möchte, den Dokumentationspflichten im Sinne der DSGVO umfassend nachzukommen.

Die Präsidentin ermuntert in einem Rundschreiben alle Beschäftigten, sich aktiv in die Pilotphase einzubringen, damit ein gangbares und effizientes Verfahren entwickelt und umgesetzt werden kann. Wenden Sie sich bei Interesse direkt an uns.

Wir weisen ausdrücklich auf die Pflichten der Verantwortlichen hin, die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO zu befolgen, der damit verbundenen Rechenschaftspflicht Genüge zu tun sowie ein Verzeichnis der Verarbeitungstätigkeiten entsprechend Art. 30 DSGVO zu führen.

Erforderlichkeit des Verzeichnisses von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten (im Folgenden kurz als „Verzeichnis“ bezeichnet) ist ein wesentliches Instrument zum Nachweis der von der Universität betriebenen und beauftragten Verarbeitungstätigkeiten personenbezogener Daten. Das betrifft neben allen IT-basierten auch die IT-losen Verarbeitungstätigkeiten, wie beispielsweise die telefonische Krankmeldung.

Da die Gesamtverantwortung für die korrekte Verzeichnisführung bei dem*der Präsident*in der TU Berlin liegt, ist die Erstellung eines Gesamtverzeichnisses adäquat.

Die dezentrale Struktur der IT an der TU stellt eine Herausforderung dar, die es dabei zu meistern gilt: Die Führungskräfte in den Fakultäten, Zentraleinrichtungen, Zentralinstituten und ZUV-Abteilungen tragen die Verantwortung für die in ihrem

Geschäftsbereich durchgeführten Verarbeitungstätigkeiten und deren Dokumentation. Die Führungskräfte können für die Verzeichnisführung Vertreter*innen benennen.

Bei der Umsetzung ist zudem zu berücksichtigen, dass unserer Aufsichtsbehörde, der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BBDI) auf Nachfrage eine Einsicht in das Verzeichnis ermöglicht werden muss.

Art und Umfang des Verzeichnisses

Das Verzeichnis wird in elektronischer Form geführt und umfasst je Verarbeitungstätigkeit zumindest die nach Art. 30 DSGVO geforderten Informationen.

Das Verzeichnis kann zudem als Verfahrensdokumentation für Beteiligungsanträge an die Personalräte oder als Ausgangspunkt für Maßnahmen zur Erhöhung der IT-Sicherheit und der Umsetzung des BSI IT-Grundschutzes[1] dienen, jedoch beschränkt sich der Fokus an dieser Stelle auf die aus der DSGVO resultierenden Pflichten.

Die gesetzlich geforderte Dokumentation von mit Dritten vereinbarten Auftragsverarbeitungsverträgen (AVVs) sowie der Vereinbarungen zur gemeinsamen Verantwortung „Joint Control“ kann ebenfalls im Verzeichnis erfolgen.

- **Zentral angebotene Verarbeitungstätigkeiten**
  Von den zentralen Bereichen der TU werden diejenigen Verarbeitungstätigkeiten im Verzeichnis dokumentiert, die für die gesamte TU angeboten und insofern standardisiert betrieben und angewandt werden. Im Kurzkonzept (Anlage 2) werden einschlägige Verarbeitungstätigkeiten genannt.
- **Eigene Verarbeitungstätigkeiten der Bereiche**
  Nur darüber hinaus gehende eigene Verarbeitungen personenbezogener Daten in den Bereichen der TU Berlin, z.B. zusätzliche Dienste und Softwareprodukte, müssen von den jeweiligen Verantwortlichen oder von ihnen benannten Vertreter*innen erfasst werden.

Dezentral geführte eigene Verzeichnisse

Wie im Rundschreiben der Präsidentin ausgeführt, ist der behördliche Datenschutz **bis zum 31.12.2022** zu informieren, sofern Bereiche bereits ein eigenes Verzeichnis führen.

Dann wird geprüft, inwieweit dieses Verzeichnis den Erfordernissen nach Art. 30 DSGVO entspricht und mit dem Bereich abgestimmt, in welcher Form es weitergeführt werden kann. In jedem Fall ist die Einsichtnahme durch den behördlichen Datenschutz und -im Falle einer Nachfrage- durch die Aufsichtsbehörde in geeigneter Form sicherzustellen.

Implementierung eines Pilotprojekts mit der TubCloud

Aus Sicht des Datenschutzes ist die Erstellung eines Gesamtverzeichnisses für die TU wünschenswert, weshalb wir seinen Aufbau im Rahmen unserer Aufsichts- und Beratungsfunktion begleiten wollen.

Hierbei wünschen wir uns eine **minimale, leichtgewichtige und flexible Lösung**, die die aus der DSGVO resultierenden Anforderungen umsetzt und eine dezentrale Pflege ermöglicht.

Es erscheint uns empfehlenswert die dezentrale Struktur der Universität adäquat im Verzeichnis abzubilden, da dieses die Dokumentation der Verarbeitungstätigkeiten durch die dezentralen Bereiche vereinfacht.

Angedacht ist ein Gesamtverzeichnis auf Basis einer Ordnerstruktur in der **TubCloud**. Diese eignet sich gut für die nach Bereichen hierarchisch strukturierte Organisationsstruktur der TU Berlin und die gemeinsame Bearbeitung von Dokumenten.

[1] s.a. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Allerdings fehlt eine strukturierte Eingabemaske - was durch das von uns entworfene Word-Template des „Datenschutz-Steckbriefs“ kompensiert werden soll. Außerdem sind die Auswertungsmöglichkeiten eingeschränkt, beispielsweise gibt es keine strukturierte Suche anhand bestimmter Kriterien (z.B. Kategorien von verarbeiteten Daten oder betroffene Personengruppen). Die Vorteile der vereinfachten Bearbeitung und die Flexibilität der TubCloud als Speicherort überwiegen jedoch aus unserer Sicht gegenüber der universitätsweiten Einführung einer spezifischen Softwarelösung.

Die Führungskräfte der Bereiche sowie die ggf. benannten Vertreter*innen werden mit entsprechenden Zugriffsrechten ausgestattet, damit sie dort die erforderlichen Informationen strukturiert einpflegen bzw. diese Aufgabe an die Führungskräfte der dezentralen Bereiche (z.B. Fachgebiete, Referate, usw.) übertragen können. Die dezentralen Bereiche können somit die von ihnen betriebenen und beauftragten Verarbeitungstätigkeiten selbst dokumentieren und haben zu jeder Zeit auch den Zugriff auf die ihren Bereich betreffenden Inhalte.

Um die Praktikabilität dieses Ansatzes zu prüfen, sollen im Rahmen der Pilotphase Erfahrungen gesammelt werden. In 2024 soll die Praxistauglichkeit des Verzeichnisses zusammen mit den neuen Chief Information Officer (CIO) und Informations-Sicherheitsbeauftragten evaluiert und Empfehlungen für das weitere Vorgehen gegeben werden.

Die angedachte Struktur ist vereinfacht in Anlage 2 beschrieben.

Das Team Datenschutz nimmt die Verzeichnispflege als festen Bestandteil in die Schulungen zum Datenschutz mit auf.

Annette Hiller, Alexander Hoffmeier, Dr. Mattis Neiling

Team Datenschutz

Anlagen:

- Anlage 1: Auszug aus der DSGVO (Art. 5, 30 und 32)
- Anlage 2: Konzept des Verzeichnisses in der TubCloud

Weitere Anlage:

- Template des Datenschutz-Steckbriefs: https://redaktion.tu.berlin/k3/datenschutz/services/downloads

Anlage 1

Auszug aus der Datenschutz-Grundverordnung DSGVO (Art. 5, 30 und 32)

KAPITEL II

Grundsätze

Artikel 5
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

(...)

KAPITEL IV

Verantwortlicher und Auftragsverarbeiter

(...)

Artikel 30
Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(...)

Artikel 32
Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(…)

Quelle: DSGVO, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679

Anlage 2

Konzept des Verzeichnisses in der TubCloud (im Pilotprojekt)

Die angedachte Struktur soll flach und damit übersichtlich bleiben, die Dokumente sollen sprechend und zur chronologischen Einordnung mit einem Datumspräfix benannt werden.

Für die Bereiche, die erstmalig das Verzeichnis nutzen wollen, wird eine Basisstruktur eingerichtet.

Struktur und Zugriffsrechte

- Ein vom Team Datenschutz verwalteter Wurzelordner in der TubCloud
- Ein- bis zweistufige Struktur je Einrichtung:
  - Ein Hauptordner je Einrichtung (Fakultät, ZE, ZI, ZUV, etc)
  - bei strukturierten Einrichtungen: Je ein Unterordner für Bereiche, die eigene Verarbeitungstätigkeiten haben; Weitere Zwischenebenen sollten im Ordner-Namen kodiert werden (z.B. Institutsname_FG-Name)
  - darin können Ordner für jede Verarbeitungstätigkeit angelegt werden
  - In diesen Ordnern werden Dokumente abgelegt, zumindest Teil 1 des Datenschutz-Steckbrief ist erforderlich
- Der Hauptordner wird mittels TubCloud -internen Teilens an die Verantwortlichen übergeben, diese können die Dokumentationspflicht an die Bereiche übertragen (über TubCloud -internes Teilen der entsprechenden Unterordner, das Teilen über im Internet frei zugängliche Links sollte nicht genutzt werden).
- Die Zugriffsrechte ergeben sich aus der hierarchischen Struktur des Verzeichnisses, das an die Struktur der TU angelehnt ist, d.h.
  - jeder Bereich hat Vollzugriff auf seinen Ordner und alle Dokumente darin,
  - die Verantwortlichen übergeordneter Bereiche auf alle ihnen zugehörigen Untereinheiten.
  - Das Team Datenschutz erhält Zugriff auf das gesamte Verzeichnis, um seiner Aufsichtspflicht nachkommen zu können.
  - Die*der Präsident*in erhält als Gesamtverantwortliche*r sowie ihre*seine Vertreter*innen erhalten bei Bedarf lesenden Zugriff.
  - Zugriffe weiterer Personen sind zunächst nicht vorgesehen.

Dokumentationsumfang

Von den Bereichen sind nur diejenigen Verarbeitungstätigkeiten anzugeben, die von ihnen selbst bzw. in ihrem Auftrag betrieben werden.

Die üblichen **allgemeinen Verarbeitungstätigkeiten** müssen nicht separat von den Bereichen dokumentiert werden. Eine Liste der allgemeinen Verarbeitungstätigkeiten soll erstellt werden, sie umfasst bspw. folgende Verarbeitungstätigkeiten:

- Verarbeitungen in den SAP-Systemen
- Annahme von Krankmeldungen
- Anwesenheitskalender (mit Outlook/Exchange)
- Bürokommunikation (E-Mail, Post, Office-Produkte)
- Lehrveranstaltungsmanagement (ISIS, Moses)
- Online-Klausuren (ISIS)
- Nutzung von Videokonferenz-Tools in der Lehre
- Dienstbesprechungen mit Videokonferenz-Tools
- Bewerbungsverfahren

Für jede dieser Verarbeitungstätigkeiten soll den TU-Mitgliedern von den fachverantwortlichen Bereichen eine Beschreibung der Verarbeitungszwecke nebst erforderlicher Sorgfaltspflichten und notwendiger Schutzmaßnahmen zur Verfügung gestellt werden (im Sinne von Handlungsanweisungen/Nutzungsbedingungen).

Eine Dokumentationspflicht ist jedoch gegeben, wenn diese Dienste abweichend der vorgesehenen bereits dokumentierten Zwecke zur Verarbeitung personenbezogener Daten genutzt werden. Als eigene Verarbeitung werden z.B. betrachtet:

- Speicherung von Teilnahme- und Notenlisten auf lokalen Rechnern bzw. Netzlaufwerken
- (Bewerbungs-)verfahren mittels Uploads, die mithilfe der TubCloud umgesetzt werden

Das Team Datenschutz berät, in welchen Fällen eine separate Dokumentation der Verarbeitung erforderlich ist.

Dokumentationsinhalte (Datenschutz-Steckbrief / Basisdokumentation)

Das Verzeichnis soll eine kompakte Basisdokumentation entsprechend der Anforderungen nach Art. 30 DSGVO liefern. Erforderlich sind in jedem Fall folgende Informationen je Verarbeitungstätigkeit:

- Name des Dienstes/der Software
- Art der Verarbeitungstätigkeit
- Ansprechpartner*in
- Verfahrensbeginn, ggf. Verfahrensende
- Zwecke der Verarbeitung, Rechtsgrundlage
- betroffene Personengruppen (deren Daten verarbeitet werden)
- Kategorien personenbezogener Daten
- Zugriffsberechtigte (innerhalb TU)
- Empfänger*innen von Datenübermittlungen (einschl. Schnittstellen)
- Übermittlung in Drittländer (nebst Dokumentierung geeigneter Garantien)
- Löschfristen
- Technische und organisatorische Maßnahmen (TOMs)

Vorgeschlagen wird, dass dafür das vom Team Datenschutz bereitgestellte Template für den Datenschutz-Steckbrief genutzt wird (s. Anlagen, elektronisch als Word-Dokument verfügbar[2]), in dem alle erforderlichen Informationen einheitlich angeben werden können.

Sofern die einzelnen Informationen zu umfangreich für eine Eintragung im Datenschutz-Steckbrief sind, kann auf separate Dokumente verwiesen werden, die ebenfalls im Verzeichnis bereitgestellt werden (z.B. ein Datenschutzkonzept). Für die verpflichtenden Informationen sollten Verweise auf Webseiten oder andere Datenspeicher vermieden werden, alle notwendigen Dokumente sollten im Verzeichnis in Kopie bereitgestellt werden ("self contained"-Ansatz; damit alle relevanten Informationen im Verzeichnis verfügbar sind).

Zusätzliche Dokumente können ebenfalls dort abgelegt werden, z.B.

- Fachkonzepte,
- Technische und organisatorische Maßnahmen (TOMs),
- Beteiligungsanträge,
- Datenschutzrechtliche Bewertungen,
- Datenschutzfolgeabschätzungen (DSFA),
- Datenschutzerklärungen,
- Beschlüsse (der Personalräte) sowie
- Kommunikation (nach Bedarf).

Zur Strukturierung und besseren Übersichtlichkeit können dafür weitere Unterordner angelegt werden. Ältere nicht mehr aktuelle Dokumente sollten im Regelfall nicht gelöscht, sondern in einen weiteren „Ablage-Unterordner“ verschoben werden um Veränderungen der Verarbeitungstätigkeit über die Zeit nachvollziehen zu können.

[2] Die jeweils aktuelle Version des Datenschutz-Steckbriefs ist als Vorlage unter „Informationen zum Download“ auf der Datenschutz-Webseite verfügbar: https://www.tu-berlin.de/asv/menue/datenschutz/informationen_zum_download/#c998603

- Idealerweise sollten die Dateinamen das Datum als Präfix enthalten und kurze sprechende Namen haben (z.B. "2021-08-13_TOMs_Mauerbau.pdf"), dazu sollen Vorschläge für Namenskonventionen erarbeitet werden.
- Das Team Datenschutz erarbeitet eine Handreichung, die beschreibt, in welchen Fällen zusätzliche Dokumente als notwendig erachtet werden (z.B. Datenschutzkonzept mit Zugriffsberechtigungen, Datenflüssen, Schnittstellen/Datenübermittlungen, Löschfristen und allgemeinen TOMs) und welche ergänzend bereitgestellt werden können (z.B. Fachkonzepte)