Multimedia Kontor Hamburg

Handreichung: Verantwortung und die damit zusammenhängenden (vertraglichen) Anforderungen gemäß der europäischen Datenschutz-Grundverordnung (DSGVO)

HINWEIS: Dieser Text dient dem Informationszweck und stellt keine Rechtsberatung dar. Es gibt keine Gewähr auf Richtigkeit oder Vollständigkeit der genannten Informationen.

Dieser Text wurde erstellt durch die Projektgruppe der Datenschutzbeauftragten der NRW-Hochschulen:

- Dr. Thilo Groll, LL.M/ Fachhochschule Dortmund, datenschutz@fh-dortmund.de
- Dr. Ursula Hilgers/ Heinrich Heine Universität Düsseldorf, datenschutz@hhu.de
- Christian Schumann/ Universität Siegen, datenschutzbeauftragter@uni-siegen.de
- Sabine Sonneborn/ Ruhr Universität Bochum, dsb@rub.de
- Dr. Britta Weber/ HS Gesundheit Bochum, dsb@hs-gesundheit.de
- Dr. Eva-Maria Wicker, LL.M/ Universität Paderborn, datenschutz@upb.de

Vorgenommene Änderungen: Entfernung der Grafischen Elemente unter III. Verantwortlichkeiten; Änderung DS-GCO in DSGVO sowie farbliche Hervorhebung einzelner Bereiche (positiv/negativ)

Inhalt

I. Vorbemerkungen

An der Verarbeitung von personenbezogenen Daten sind häufig unterschiedliche Akteure beteiligt. In Kooperationen wirken z.B. unterschiedliche Hochschulen und/oder Unternehmen zusammen oder bei der Durchführung von Studien oder der Beschaffung von Arbeitsmitteln (z. B. Software) werden Dienstleister einbezogen. Werden bei der Zusammenarbeit in Kooperationen personenbezogene Daten verarbeitet, stellt sich stets die Frage, wer für welche Verarbeitung personenbezogener Daten verantwortlich ist und wer welche datenschutzrechtlichen Pflichten zu erfüllen hat. Dieses Handout gibt einen Überblick über die unterschiedlichen Verantwortlichkeiten und ihre wesentlichen (vertraglichen) Anforderungen im Rahmen der Verarbeitung personenbezogener Daten gemäß den Vorgaben der Datenschutz-Grundverordnung (DSGVO).

Hinweis: Die Handreichung thematisiert an dieser Stelle nicht die Bedeutung der Verantwortlichkeit im Wissenschaftsbereich, wo die Forschung im Hauptamt betrieben wird. Es gibt Stimmen, die sagen, dass die Datenverarbeitung insgesamt in der alleinigen Verantwortung der Hochschule liege, es gibt aber auch eine Ansicht die sagt, dass die Hochschulen bei Forschungsvorhaben gar nicht Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO sind, denn über Zwecke und Mittel der Datenverarbeitung entscheiden nach deren Auffassung alleine die Wissenschaftler*innen und zwar in Ausübung ihres höchstpersönlichen Grundrechts auf Wissenschaftsfreiheit (Art. 5 Abs. 3 GG)[1].

II. Personenbezogene Daten als Ausgangspunkt für datenschutzrechtliche Verantwortung

Die Einhaltung des Datenschutzes spielt immer (nur) dann eine Rolle, wenn personenbezogene Daten von natürlichen Personen verarbeitet werden, also z. B. von Angehörigen oder Mitgliedern einer Hochschule oder weiteren Dritten (z.B. Proband*innen, Industriepartnern).

Personenbezogene Daten sind gemäß Artikel 4 Nummer 1 der DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Beispiele für personenbezogene Daten sind:

- **Allgemeine Personen- und Kontaktdaten** (Name, Geburtsdatum/Alter, Geburtsort, Anschrift, (E- Mail-) Adresse, Telefonnummer/n)
- …

Kennnummern
- Matrikelnummer
- Sozialversicherungsnummer
- Steueridentifikationsnummer
- Nummer bei der Krankenversicherung
- Personalausweisnummer
- …

Physische Merkmale
- Geschlecht
- Haut-, Haar- und Augenfarbe
- Statur/Gewicht
- Kleidergröße
- …

[1] Schwartmann, Rolf, in: Ordnung der Wissenschaft (2/2020), Die Verantwortlichkeit für die Verarbeitung von Forschungsdaten an Hochschulen; Seite 77, 84.

Bankdaten
- Kontonummern
- Kreditinformationen
- Kontostände
- …

Online-Daten
- IP-Adresse
- Standortdaten
- …

Forschungsdaten
- Umfragedaten,
- Texte,
- Audio- und Videodateien
- …

Werturteile
- Zeugnisse
- Prüfungsleistungen
- …
-

Demografische Daten
- Alter
- Geschlecht
- Familienstand
- Einkommen
- Bildung und Beschäftigungsstatus
- …

Eigentums- und Besitzmerkmale
- Fahrzeug- und Immobilieneigentum
- Grundbucheintragungen
- Kfz-Kennzeichen
- Zulassungsdaten
- …

Sensible Daten (gemäß Artikel 9 DSGVO)
- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit
- genetische Daten[2]
- biometrische Daten zur eindeutigen Identifizierung einer Person[3]
- Gesundheitsdaten[4]
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Eine Verarbeitung personenbezogener Daten ist gemäß Artikel 4 Nummer 2 DSGVO jeder Vorgang im Zusammenhang mit dem Erheben, dem Erfassen, der Organisation, dem Ordnen, der Speicherung, der Anpassung oder Veränderung, dem Auslesen, dem Abfragen, der Verwendung, der Offen-legung durch Übermittlung, der Verbreitung oder eine andere Form der Bereitstellung, dem Abgleich oder der Verknüpfung, der Einschränkung, dem Löschen oder der Vernichtung von personenbezogenen Daten.

Wichtig: Der Schutz personenbezogener Daten erstreckt sich nicht nur auf digitale Formate. Er bezieht sich auf eine ganz oder teilweise automatisierte sowie auf eine nichtautomatisierte Verarbeitung personenbezogener Daten, sofern diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Das Dateisystem muss nicht digital sein.

[2] Personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.
[3] Mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.
[4] Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

III. Verantwortlichkeiten

1. Alleinige Verantwortung

Die datenschutzrechtliche Verantwortung i.S.d. DSGVO begründet sich dadurch, dass eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Artikel 4 Nummer 7 DSGVO). Wirken mehrere Akteure zusammen, entscheidet allerdings jeder allein über Zweck und Mittel, trägt jeder Akteur die alleinige Verantwortung. Typisch für eine alleinige Verantwortung sind etwa Verarbeitungen von personenbezogenen Daten im Rahmen von Vertragsbeziehungen, die Übermittlung von personenbezogenen Daten an Sozialversicherungsträger oder die gemeinsame Nutzung einer IT-Infrastruktur mit separaten Instanzen.

Beispiel: Drei Hochschulen betreiben gemeinsam die Infrastruktur für ein Campus-Management. Hinsichtlich der im System verarbeiteten Beschäftigen- und Studierendendaten wird jedoch jeweils eine Verarbeitung in alleiniger Verantwortung durch die jeweilige Hochschule vorliegen, weshalb bezüglich dieser Daten auch eine Verarbeitung in getrennten Instanzen vorgesehen werden muss.

Anforderungen:

Der Alleinverantwortliche hat das vollständige Pflichtenprogramm der DSGVO zu erfüllen (Artikel 5, 24 DSGVO). Insbesondere hat er eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten sicherzustellen, die betroffenen Personen im Rahmen der Transparenzpflichten zu informieren (Artikel 13 DSGVO) sowie die Dokumentationspflichten sicherzustellen (Artikel 30 DSGVO).

2. Gemeinsame Verantwortung gemäß Art. 26 DSGVO

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche (Artikel 26 Abs. 1, S. 1 DSGVO). Als Zweck ist das Warum (Ziel, Ergebnis usw.), und als Mittel das Wie (auf welche Art und Weise wird ein Ziel, Ergebnis etc. erreicht?) der Verarbeitung personenbezogener Daten zu verstehen. Eine gemeinsame Verantwortung setzt nicht voraus, dass jeder der Verantwortlichen identische Handlungsoptionen hat und die Verantwortung zu gleichen Teilen gegeben ist (EuGH, C-40/17 Rn. 70). Ein faktischer Einfluss auf Steuerung und Kontrolle der Datenverarbeitung genügt. So reicht es z.B. aus, dass sich ein Forschungspartner an der Verarbeitung eines anderen Forschungspartners beteiligt und diese strukturell fördert oder ermöglicht (siehe Frauenhofer, Guide, Leitlinien Datenschutz in der wissenschaftlichen Forschung, 2019, S. 6). Auch der tatsächliche Zugang zu den Daten ist kein maßgebliches Kriterium (EuGH, C-40/17 Rn. 69). Die Zwecke zwischen den Verantwortlichen können auch verschieden sein, müssen sich aber ergänzen. Liegt eine gemeinsame Verantwortung vor, bedarf es einer speziellen Vereinbarung gemäß Artikel 26 Abs. 1 und Abs. 2 DSGVO, welche bestimmte Anforderungen erfüllen muss. Die Vereinbarung muss transparent und wahr sein sowie eine eindeutige Verantwortungs- und Pflichtenaufteilung aufzeigen, wobei die Pflichtenaufteilung zur Disposition steht, soweit es keine festgelegten unions- oder mitgliedstaatlichen Vorgaben gibt. Insofern kann die Durchführung eines gemeinsamen Forschungsprojektes, an dem unterschiedliche Forschungspartner (auch aus der Industrie z.B.) mitwirken, durchaus eine gemeinsame Verantwortung begründen. Eine Vereinbarung allein begründet nicht bereits eine gemeinsame Verantwortung. Sie kann nur an den tatsächlichen Umständen (wie zuvor beschrieben) beurteilt werden.

Beispiele für eine gemeinsame Verantwortung sind:[5]

- klinische Arzneimittelstudien
- gemeinsame Nutzung einer Datenbank; gemeinsame Errichtung einer Infrastruktur, auf der mehrere Beteiligte ihre jeweils individuellen Zwecke verfolgen, z.B. gemeinsames Betreiben einer internetgestützten Plattform
- gemeinsame Verwaltung bestimmter Datenkategorien (z.B. Adressdaten)
- gemeinsame Durchführung von Umfragen mit gemeinsamer Ergebnispartizipation (z.B. statistische Auswertungen)

Beispiele: Keine gemeinsame Verantwortung

- Verantwortlicher hat (selbst) einen gesetzlichen Auftrag zu Erfüllung bestimmter Aufgaben (z.B. ausgelagerte Beihilfeabrechnungen durch Sozialträger, Zusammenarbeit mit Stiftung für Hochschulzulassung etc.)

Anforderungen:

Liegt eine gemeinsame Verantwortung vor, benötigt ebenso wie bei der alleinigen Verantwortung jeder der gemeinsam Verantwortlichen seine eigene **Rechtsgrundlage** für die Verarbeitung personenbezogener Daten, inklusive der Übermittlung an die anderen gemeinsamen Verantwortlichen und kann sich somit nicht auf die einem anderen (Vertrags-)Partner zustehende Rechtsgrundlage berufen.

Es muss zudem eine **Vereinbarung** zwischen den beteiligten (Vertrags-) Partnern gemäß den Anforderungen des Artikel 26 Abs. 1 und Abs. 2 DSGVO geschlossen werden, der die gemeinsame Verantwortlichkeit und die sich daraus ergebenden Rechte und Pflichten regelt. Das Pflichtenprogramm kann dabei gemäß Artikel 26 DSGVO unterschiedlich ausgestaltet werden.[6]

Besondere Anforderungen bestehen im Rahmen der gemeinsamen Verantwortung an die **Informationspflicht**. Die betroffenen Personen sind *neben den allgemeinen Anforderungen (s.o.)* über die gemeinsame Verantwortung aufzuklären, dabei ist auch das Wesentliche der Vereinbarung zur Verfügung zu stellen.[7]

3. Auftragsverarbeitung gemäß Artikel 28 DSGVO

Bei der Auftragsverarbeitung wird eine externe Stelle in die von allein oder gemeinsam Verantwortliche stattfindende Verarbeitung personenbezogener Daten eingebunden. Dies kann z.B. bei der Auslagerung des Serverbetriebs an eine andere Stelle der Fall sein. Der wesentliche Unterschied zur alleinigen und gemeinsamen Verantwortung besteht darin, dass der eingebundene Dienstleister einem umfänglichen Weisungsrecht des Auftraggebers unterliegt. Bei der Auftragsverarbeitung besteht somit ein Über-/Unterordnungsverhältnis zwischen Auftraggeber (Verantwortlicher) und Auftragnehmer (Auftragsverarbeiter). Ein Auftraggeber bleibt hinsichtlich der Verarbeitung im Auftrag Verantwortlicher i. S. d. DSGVO und unterstellt den Auftragnehmer seiner Kontrolle und seinen Anweisungen in Bezug auf die Verarbeitung der personenbezogenen Daten.

Eine Auftragsverarbeitung liegt grundsätzlich immer dann vor, wenn durch die externen Stellen/Dienstleister eine Verarbeitung personenbezogener Daten Schwerpunkt eines Auftrags/Vertrags ist.

[5] Vgl. DSK Kurzpapier Nr. 16 „Gemeinsam für Datenverarbeitung Verantwortliche“, www.datenschutzkonferenz-online.de/kurzpapiere.html.
[6] Siehe „Formular Gemeinsame Verantwortlichkeit“ mit den Anlagen 1 und 2 zu finden in der Infothek des Datenschutzportals.
[7] Siehe Fußnote 11 im o.g. „Formular Gemeinsame Verantwortlichkeit“.

Beispiele für eine Auftragsverarbeitung sind:[8]

- Bereitstellung IT- Dienstleistungen oder Software (E-Mail-Versand, Hosting von Internetseiten, Webtracking, Newsletterversand, Support an Internetseiten/Software, (Fern-)Wartungen von Servern, auf IT-Geräten etc., Datenbanken, Cloudsystem, Datenerfassung, Datenkonvertierung, Backup Sicherungen, Umfragetools/ -software/ -plattformen)
- Aufträge an Befragungsinstitute
- Aufträge an Transkriptionsbüros
- Vernichtung von Datenträgern
- Aufträge an Druckereien
- Unterstützung von Verwaltungssystemen

Beispiele: Keine Auftragsverarbeitung

Berufsgeheimnisträger (RAe, Wirtschaftsprüfer, externe Betriebsärzte)

Anforderungen:

1. Bei einer Auftragsverarbeitung gemäß Artikel 28 DSGVO wird grundsätzlich keine weitere **Rechtsgrundlage** für die Übermittlung an den Auftragsverarbeiter und für die weitere Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter erforderlich (Ausnahme: Übermittlung in Drittstaat), da die Auftragsverarbeitung (wenn auch umstritten) als privilegiert gilt. Maßgeblich ist daneben jedoch die Rechtsgrundlage, auf die sich die Hochschule selbst stützt.
2. Jedoch muss für die Übermittlung an den Auftragsverarbeiter und für die weitere Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter ein **Vertrag** mit den inhaltlichen Mindestvoraussetzungen aus Artikel 28 Abs. 3 DSGVO geschlossen werden, der die weitere Wahrnehmung der Verantwortlichkeit und die Sicherstellung der Verarbeitung personenbezogener Daten durch den Auftraggeber gewährleistet.
3. *den allgemeinen Anforderungen (s.o.)*

Wichtig: Liegt keine Weisungsgebundenheit vor, handelt es sich um eine Verarbeitung als Verantwortlicher und nicht als Auftragsverarbeiter.

IV. Zusätzliche Anforderungen an die Übermittlung von personenbezogenen Daten an Drittländer

Bei einer Verarbeitung von personenbezogenen Daten außerhalb der EU hat ein Verantwortlicher zusätzlich die Anforderungen der Art. 44 ff. DSGVO einzuhalten. Damit kann auch die Umsetzung von weiteren vertraglichen Anforderungen verbunden sein. Dies ist insbesondere dann der Fall, wenn das Drittland, an das personenbezogene Daten übermittelt werden sollen, nicht unter die Liste der Angemessenheitsbeschlüsse der EU-Kommission fällt und auch keine weiteren sog. geeigneten Garantien gemäß Art. 46 DSGVO (z.B. Binding Corporate Rules gemäß Art. 46 Abs. 2 lit. b) i.V.m. Art. 47 DSGVO) oder – in seltenen Fällen – Ausnahmen für bestimmte Fälle gemäß Art. 49 DSGVO vorliegen.

Häufiger Anwendungsfall ist insoweit der Abschluss von Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO.

[8] Vgl. DSK- Kurzpapier Nr. 13 „Auftragsverarbeitung Art. 28 DSGVO“, www.datenschutzkonferenz-online.de/kurzpapiere.html.

Mit dem Abschluss von Standarddatenschutzklauseln ist die Sicherstellung einer Reihe von Anforderungen verbunden. Während zunächst das für die Übermittlung einschlägige Modul auszuwählen ist, umfasst die mit dem Abschluss der Klauseln durchzuführende Prüfung insbesondere die Bewertung des Datenschutzniveaus bzw. der Rechtslage im Zielland. Insofern ergeben sich folgende Schritte:

1. Auswahl des richtigen Moduls

Standardvertragsklauseln gibt es für unterschiedliche Verarbeitungssituationen. Diese sind:

Modul 1: Übermittlung von Verantwortlichen an Verantwortliche

Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter

Modul 3: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

Modul 4: Übermittlung von Auftragsverarbeitern an Verantwortliche

Die häufigsten Anwendungsfälle für Hochschulen sind die Verarbeitungssituationen der Module 1 und 2.

Wichtiger Hinweis: Bei Verwendung von Modul 2 (Auftragsverarbeitungen) sind die Anforderungen für Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO bereits von den Standarddatenschutzklauseln mitabgedeckt, sodass in diesen Fällen kein separater Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DSGVO abzuschließen ist.

2. Durchführung eines Transfer Impact Assessment (TIA)

Mit dem Abschluss von Standarddatenschutzklauseln verbunden ist gem. der Klausel 14 der Standarddatenschutzklauseln insbesondere die Durchführung eines sog. Transfer Impact Assessment (TIA). Gegenstand der TIA ist eine Bewertung, ob das Datenschutzniveau im Drittland im Sinne der DSGVO angemessen ist. Es obliegt dem Exporteur/ Importeur der personenbezogenen Daten zu prüfen/ zu gewährleisten, dass das Datenschutzniveau im Drittland dem der EU vergleichbar ist und praktisch auch umgesetzt wird. Hierzu sind unterschiedliche Prüfkriterien zu beachten.

Sofern festgestellt wird, dass im Zielland (d. h. im Drittland des Datenimporteurs) ein rechtmäßiger Zugriff auf die Daten gegeben ist, der innerhalb der EU verboten wäre, sind eine weitere Risikoabschätzung vorzunehmen sowie bestimmte Absicherungen durch den Datenimporteur erforderlich (Klausel 15). (Auch) Die TIA hat in jedem Einzelfall unter Einbindung der*des zuständigen Daten-schutzbeauftragten zu erfolgen.