 

  DFN-CERT Services GmbH Logo

Datenschutzkonzept nach   
den Anforderungen der DS-GVO

Version 2.0, 3. Mai 2019

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz CC BY-SA 3.0   
<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>   
Autor: NRW Projektgruppe „Umsetzung der EU-Datenschutz-Grundverordnung (DS-GVODS-GVO) −  
Datenschutzmanagementsysteme“ 2018

gefördert vom 

Inhalt

[Wirksame Zielsetzung 5](#_Toc8391728)

[I. Gesetzliche Vorgaben zum Datenschutz 5](#_Toc8391729)

[EU-Datenschutzgrundverordnung (DS-GVO) 5](#_Toc8391730)

[Bundesdatenschutzgesetz (BDSG) 5](#_Toc8391731)

[Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) 6](#_Toc8391732)

[Gesetz über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG NRW) 6](#_Toc8391733)

[Einschreibungsordnung der Hochschule gem. § 48 Abs. 1 S. 3 HG NRW 6](#_Toc8391734)

[Drittes Gesetz über die Zulassung zum Hochschulstudium in Nordrhein-Westfalen (Hochschulzulassungsgesetz – HZG) 6](#_Toc8391735)

[Landeshaushaltsordnung (LHO) 6](#_Toc8391736)

[Beamtenstatusgesetz (BeamtStG), Landesbeamtengesetz (LBG NRW) 7](#_Toc8391737)

[Tarifverträge, Dienstvereinbarungen 7](#_Toc8391738)

[Gesetz über die Statistik für das Hochschulwesen sowie für die Berufsakademien (HStatG) 7](#_Toc8391739)

[Telekommunikationsgesetz (TKG) 7](#_Toc8391740)

[II. Materielle Anforderungen an die Datenschutzorganisation 7](#_Toc8391741)

[Bekenntnis der Leitungsebene zum Datenschutz, Förderung einer Datenschutz- und Sicherheitskultur (Art. 24, 26) 7](#_Toc8391742)

[Organisatorische Gewährleistung Verzeichnis von Verarbeitungstätigkeiten (Art. 30) 7](#_Toc8391743)

[Gesetzliche Anforderungen für Verantwortliche an das Verzeichnis von Verarbeitungstätigkeiten 8](#_Toc8391744)

[Über Art. 30 Abs. 1 DS-GVO hinausgehende Angaben 10](#_Toc8391745)

[Gesetzliche Anforderungen für Auftragsverarbeiter an das Verzeichnis von Verarbeitungstätigkeiten 10](#_Toc8391746)

[Abgrenzung zu beschreibender Verarbeitungen 10](#_Toc8391747)

[Zuständigkeit/Verantwortlichkeit 11](#_Toc8391748)

[Umsetzung 12](#_Toc8391749)

[Aufarbeitung des bestehenden Rückstands 13](#_Toc8391750)

[Organisatorische Gewährleistung der Umsetzung verarbeitungsbezogener Anforderungen (Art. 5 Abs. 1) 13](#_Toc8391751)

[Hochschulleitung 13](#_Toc8391752)

[Stabsstelle Datenschutz 14](#_Toc8391753)

[Verfahrensverantwortlicher 14](#_Toc8391754)

[Beschäftigte 15](#_Toc8391755)

[Datenschutz- und Informationssicherheits-Koordinatorinnen / -koordinatoren 15](#_Toc8391756)

[Behördliche Datenschutzbeauftragte / Behördlicher Datenschutzbeauftragter 15](#_Toc8391757)

[Informationssicherheitsbeauftragte / Informationssicherheitsbeauftragter 16](#_Toc8391758)

[Effektive Datenschutzkontrolle (Art. 37 -39) 16](#_Toc8391759)

[Angemessene Maßnahmen für die Sicherheit personenbezogener Daten (Art. 32) 17](#_Toc8391760)

[Informationssicherheit und Art. 32 DS-GVO 17](#_Toc8391761)

[Vorrang technischer Maßnahmen 17](#_Toc8391762)

[Stand der Technik 18](#_Toc8391763)

[Basis-Sicherheit 18](#_Toc8391764)

[Schwellwertanalyse und Schutzbedarfsfeststellung 19](#_Toc8391765)

[Risikoanalyse/Datenschutzfolgeabschätzung (DSFA) 19](#_Toc8391766)

[Strukturelle Gewährleistung der Betroffenenrechte (Art. 12 – 22) 20](#_Toc8391767)

[Rechtliche Grundlage 20](#_Toc8391768)

[Umsetzung der Informationspflicht bei der Erhebung 22](#_Toc8391769)

[Information bei der Erhebung bei Dritten (Art. 14) 24](#_Toc8391770)

[Umsetzung der Informationspflicht 25](#_Toc8391771)

[Auskunft (Art. 15) 25](#_Toc8391772)

[Berichtigung (Art. 16) 26](#_Toc8391773)

[Löschung und Recht auf Vergessenwerden (Art. 17) 26](#_Toc8391774)

[Einschränkung der Verarbeitung (Art. 18) 27](#_Toc8391775)

[Datenübertragbarkeit (Art. 20) 27](#_Toc8391776)

[Widerspruch (Art. 21) 28](#_Toc8391777)

[Automatisierte Entscheidung im Einzelfall (Art. 22) 28](#_Toc8391778)

[Verantwortlichkeit / Zuständigkeit 29](#_Toc8391779)

[Identität des Betroffenen und Authentizität der Anfrage 29](#_Toc8391780)

[Technische Maßnahmen zur Gewährleistung der Betroffenenrechte 30](#_Toc8391781)

[Ablehnung, Fristverlängerung und Information hierüber 30](#_Toc8391782)

[Kontrolle und Überwachung der Gewährleistung der Betroffenenrechte 31](#_Toc8391783)

[Strukturelle und organisatorische Sicherstellung der Meldepflichten aus Art. 33 und 34 DS-GVO 31](#_Toc8391784)

[Rechtliche Grundlagen 31](#_Toc8391785)

[Verantwortlichkeiten 32](#_Toc8391786)

[Technische und organisatorische Maßnahmen 33](#_Toc8391787)

[Information und Schulung der Mitarbeiter (Art. 29) 33](#_Toc8391788)

[Strukturelle und organisatorische Sicherstellung der Erfüllung der Anforderungen an Auftragsverarbeitungen 34](#_Toc8391789)

[Strukturelle und organisatorische Sicherstellung der Erfüllung der Anforderungen bei einer Übermittlung von personenbezogenen Daten in Drittstaaten 36](#_Toc8391790)

[Angemessenheitsbeschluss 37](#_Toc8391791)

[Einwilligung des Betroffenen 37](#_Toc8391792)

[Angemessenheitsbeschlüsse mit Prüfungsbedarf, Übermittlungen vorbehaltlich geeigneter Garantien, weitere Ausnahmen im Einzelfall nach Art. 49 37](#_Toc8391793)

[Bestandsverarbeitungen 38](#_Toc8391794)

[Datenschutz-Folgenabschätzung (DSFA) 38](#_Toc8391795)

[III. Verarbeitungsbezogene Gewährleistung der Anforderungen 38](#_Toc8391796)

[Verantwortliche Stelle 38](#_Toc8391797)

[Zweck der Verarbeitung 39](#_Toc8391798)

[Rechtsgrundlage (Art. 5 Abs. 1 a) a.) 39](#_Toc8391799)

[Gewährleistungsziel Datensparsamkeit (Art. 5 Abs. 1 a) a.) 39](#_Toc8391800)

[Gewährleistungsziel Transparenz (Art. 5 Abs. 1 a) b., c. und d.) 39](#_Toc8391801)

[Gewährleistungsziel Verfügbarkeit (Art. 5 Abs. 1 f)) 39](#_Toc8391802)

[Gewährleistungsziel Integrität (Art. 5 Abs. 1 d) und f)) 39](#_Toc8391803)

[Gewährleistungsziel Vertraulichkeit (Art. 5 Abs. 1 f)) 40](#_Toc8391804)

[Gewährleistungsziel Nichtverkettbarkeit (Art. 5 Abs. 1 b), c) und e)) 40](#_Toc8391805)

[Gewährleistungsziel Intervenierbarkeit (Art. 5 Abs. 1 d) und e)) 40](#_Toc8391806)

[IV. Weiterentwicklung des Ansatzes zum Datenschutzmanagement 40](#_Toc8391807)

[Plan: Planungsphase 40](#_Toc8391808)

[Do: Umsetzungsphase 41](#_Toc8391809)

[Check: Überprüfungsphase 41](#_Toc8391810)

[Act: Anpassungsphase 41](#_Toc8391811)

[V. Umgang mit Anfragen von Sicherheits- und Strafverfolgungsbehörden 41](#_Toc8391812)

[Anfragen von Strafverfolgungsbehörden 42](#_Toc8391813)

[Sicherheitsbehörden und Geheimdienste 42](#_Toc8391814)

[Prozessuale Sicherstellung der Zulässigkeit der Verarbeitung 43](#_Toc8391815)

[Erhalt der Anfrage/Aufforderung 43](#_Toc8391816)

[Bearbeitung 44](#_Toc8391817)

[Auskunfterteilung /Zurverfügungstellung der Informationen /Duldung von Maßnahmen 44](#_Toc8391818)

[Zusammenfassung von Kernaktivitäten 45](#_Toc8391819)

# Wirksame Zielsetzung

Die Einhaltung der Anforderungen aus der EU-Datenschutzgrundverordnung (DS-GVO), den weiter geltenden bereichsspezifischen Regelungen und den landesgesetzlichen Umsetzungen der Öffnungsklauseln muss durch organisatorische, prozessuale und technische Maßnahmen nachweisbar sichergestellt werden. Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO beinhalten eine Rechenschaftspflicht, nach der die datenverarbeitende Stelle nachweisen können muss, dass die Verarbeitung von personenbezogenen Daten unter Einhaltung der Datenschutzbestimmungen aus Art. 5 Abs. 1 der DS-GVO und den weiteren konkretisierenden Vorgaben aus der DS-GVO und dem Landesrecht erfolgt.

Die nachweisbare Sicherstellung orientiert sich hierbei an den materiellen Anforderungen der maßgeblichen Datenschutzgesetze. Diese enthalten sowohl übergeordnete Anforderungen an die Datenschutzorganisation als auch materielle Anforderungen an die Datenschutzkonformität konkreter Verarbeitungen. Durch das vorliegende Konzept soll die technische und organisatorische Umsetzung dieser Anforderungen in der Hochschule gewährleistet werden.

Damit die rechtlichen, technischen und organisatorischen Anforderungen dauerhaft erfüllt werden können, muss zudem ein Managementsystem zur kontinuierlichen Verbesserung der Datenschutzorganisation und -maßnahmen installiert werden (vgl. Art. 32 Abs. 1 lit. d DS-GVO).

# Gesetzliche Vorgaben zum Datenschutz

Folgende gesetzlichen Vorgaben zum Datenschutz gelten für die Hochschule:

## EU-Datenschutzgrundverordnung (DS-GVO)

Die Datenschutzgrundverordnung (DS-GVO) gilt seit dem 25.05.2018 in allen Mitgliedstaaten der Europäischen Union als unmittelbar geltendes Recht, ohne dass es wie bei bisherigen Richtlinien einer mitgliedstaatlichen Umsetzung bedarf. Die DS-GVO gilt prinzipiell auch im öffentlichen Bereich und somit auch für die Hochschule als öffentliche Körperschaften des Landes NRW. Es besteht ein Geltungsvorrang der DS-GVO gegenüber Landes- und Bundesrecht, sodass prinzipiell die DS-GVO vorrangig gilt. Allerdings enthält die DS-GVO zahlreiche Öffnungsklauseln, die ergänzende und näher ausgestaltende Regelungen durch die Mitgliedstaaten zulassen. Eine sehr wichtige diesbezügliche Öffnungsklausel ergibt sich aus Art. 6 Abs. 2 und 3 DS-GVO, die den Mitgliedstaaten für ihren öffentlichen Bereich sehr weitgehende Regelungsbefugnisse gibt. Der Bund und die Länder können und müssen daher ihre bisherige Gesetzgebung mit Bezug zum Datenschutz anpassen. Soweit keine spezielleren oder abweichenden Regelungen des Bundes oder der Länder aufgrund der Öffnungsklauseln bestehen, findet die DS-GVO Anwendung.

## Bundesdatenschutzgesetz (BDSG)

Das bisherige Bundesdatenschutzgesetz (BDSG) wurde 2017 durch das Datenschutzanpassungs- und Umsetzungsgesetz (DSAnpUG) an die DS-GVO angepasst. In diesem Zuge wurden auch Umsetzungen aufgrund von Öffnungsklauseln vorgenommen. Die dabei entstandene Neufassung des BDSG gilt wie die DS-GVO ab dem 25.05.2018. Neben der Geltung für öffentliche Stellen des Bundes, wurden auch Öffnungsklauseln für den privaten Bereich umgesetzt, insbesondere mit Blick auf die Betroffenenrechte, die Möglichkeit zur Verarbeitung besonderer Kategorien von personenbezogenen Daten und den Beschäftigtendatenschutz. Das BDSG findet auf die Hochschule nur insoweit Anwendung, als sie sich privatrechtlich im Wettbewerb betätigt und dabei keine Aufgaben nach § 3 HG NRW wahrnimmt (§ 5 Abs. 5 Nr. 4 S. 2 DSG NRW). Im Übrigen findet das BDSG auf Ausgründungen und An-Institute in privatrechtlicher Rechtsform (z. B. UG haftungsbeschränkt, GmbH, AG, etc.) Anwendung. Für die Wahrnehmung aller öffentlichen Aufgaben findet auf die Hochschule das DSG NRW Anwendung.

## Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)

Der nordrhein-westfälische Gesetzgeber hat das DSG NRW aus dem Jahr 2000 mit dem Nordrhein-Westfälischen Datenschutz-Anpassungs- und Umsetzungsgesetz EU (NRWDSAnpUG-EU) an die DS-GVO angepasst. Seit dem 25.05.2018 gilt das DSG NRW n. F. Alle folgenden Bezugnahmen auf das DSG NRW beziehen sich auf das DSG NRW n.F. Neben den notwendigen terminologischen Anpassungen wurde insbesondere auch von der Öffnungsklausel aus Art. 6 Abs. 2 und 3 DS-GVO Gebrauch gemacht und zahlreiche Regelungen zur Verarbeitung von personenbezogenen Daten durch öffentliche Stellen in NRW geschaffen. So bestimmt § 3 Abs. 1 DSG NRW: „Soweit spezialgesetzliche Regelungen nicht vorgehen, ist die Verarbeitung personenbezogener Daten zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe der verarbeitenden Stelle erforderlich ist“. Diese Umsetzung schafft somit neben der Wiederholung von Art. 6 Abs. 1 Buchstabe e) DS-GVO den Raum für die Anwendung bereichsspezifischer Datenschutzregelungen aus dem Landesrecht, wie z. B. aus dem Hochschulgesetz. Das DSG NRW findet im Rahmen der Öffnungsklausel neben der DS-GVO Anwendung auf die öffentlichen Stellen des Landes NRW und somit auch auf die Hochschule. Konkret sind hier die Vorschriften in § 17 DSG NRW zur Verarbeitung personenbezogenen Daten zu wissenschaftlichen und historischen Forschungszwecken sowie zu statistischen Zwecken, in § 18 zur Datenverarbeitung im Beschäftigungskontext sowie § 19 zur Verarbeitung zu künstlerischen und literarischen Zwecken zu nennen.

## Gesetz über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG NRW)

Das Hochschulgesetz (HG) enthält spezialgesetzliche Bestimmungen zur Verarbeitung von personenbezogenen Daten durch Hochschulen. Eine explizite Regelung zum Datenschutz befindet sich in § 8 HG, in der unter anderem die Übermittlung von Daten an das Ministerium, die Verarbeitung zu Evaluationszwecken und zur Kontaktpflege mit Ehemaligen geregelt ist. Darüber hinaus finden sich verteilt über das HG weitere Bestimmungen zur Zulässigkeit der Verarbeitung von personenbezogenen Daten von Mitgliedern und Angehörigen der Hochschule. So enthält § 48 Abs. 1 S. 2 HG eine gesetzliche Ermächtigung zu Einschreibeordnungen der Hochschulen, in denen gemäß S. 3 Bestimmungen zu den zu verarbeitenden Daten getroffen werden können.

## Einschreibungsordnung der Hochschule gem. § 48 Abs. 1 S. 3 HG NRW

In der aufgrund von § 48 Abs. 1 S. 3 HG erlassenen Einschreibungsordnung der Hochschule ist bestimmt, welche personenbezogenen Daten von Studierenden verarbeitet werden.

## Drittes Gesetz über die Zulassung zum Hochschulstudium in Nordrhein-Westfalen (Hochschulzulassungsgesetz – HZG)

Das Hochschulzulassungsgesetz (HZG) enthält in § 6 eine Ermächtigung zum Erlass von Verordnungen zur Vergabe von Studienplätzen. Die aufgrund dessen erlassene Vergabeverordnung NRW (VergabeVO NRW) enthält unter anderem die gesetzlichen Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten von Bewerbern im Rahmen des Dialogorientierten Serviceverfahrens (DOSV) im Rahmen von „Hochschulstart“.

## Landeshaushaltsordnung (LHO)

Die Landeshaushaltsordnung enthält Bestimmungen aus denen sich das Erfordernis der Verarbeitung von personenbezogenen Daten im Rahmen der Rechnungslegung und Buchführung ergibt. Sie begründen somit in den relevanten Fällen die Erforderlichkeit zur Verarbeitung von personenbezogenen Daten im Rahmen der Aufgabenerfüllung der Hochschule.

## Beamtenstatusgesetz (BeamtStG), Landesbeamtengesetz (LBG NRW)

Diese Gesetze enthalten Bestimmungen über die Führung von Personalakten für beamtete Beschäftigte in NRW. § 18 Abs. 5 DSG NRW bestimmt, dass diese Vorgaben auch auf nicht beamtete Beschäftigte Anwendung finden.

## Tarifverträge, Dienstvereinbarungen

§ 18 Abs. 1 DSG NRW bestimmt, dass sich Rechtsgrundlagen für die Zulässigkeit der Verarbeitung personenbezogener Daten im Beschäftigungskontext auch aus Tarifverträgen und Dienstvereinbarungen ergeben können.

## Gesetz über die Statistik für das Hochschulwesen sowie für die Berufsakademien (HStatG)

Das Gesetz über die Statistik für das Hochschulwesen sowie für die Berufsakademien verlangt von den Hochschulen teils Angaben die über die sonstigen Erfordernisse der Bewerber-, Studierenden- und Prüfungsverwaltung hinausgehen

## Telekommunikationsgesetz (TKG)

Soweit die Privatnutzung durch Beschäftigte und Studierende nicht wirksam ausgeschlossen ist, finden auf die Kommunikationsdienste Internet, E-Mail und Telefonie/Telefax die Datenschutzbestimmungen des Telekommunikationsgesetzes für geschäftsmäßige Anbieter von Telekommunikation Anwendung.

# Materielle Anforderungen an die Datenschutzorganisation

Ziel ist die Schaffung einer Datenschutzorganisation, die die Erfüllung der Anforderungen der DS-GVO nachweisbar gewährleistet. Die DS-GVO stellt nicht nur Anforderungen in Bezug auf konkrete Verarbeitungen von personenbezogenen Daten. Es werden darüber hinaus Anforderungen an die Organisation von verantwortlichen Stellen gestellt, damit der Schutz der Grundrechte betroffener Personen tatsächlich und fristgerecht gewährleistet werden kann. Das Konzept beschäftigt sich nachfolgend mit diesen verarbeitungsübergreifenden Anforderungen an die Datenschutzorganisation der Hochschule.

## Bekenntnis der Leitungsebene zum Datenschutz, Förderung einer Datenschutz- und Sicherheitskultur (Art. 24, 26)

Mit der geltenden Leitlinie vom <TT.MM.JJJJ> der Hochschule besteht eine für die Hochschule und ihre Angehörigen, Mitglieder und Beschäftigten verbindliche Vorgabe für den Datenschutz als wichtiges Organisationsziel zum Grundrechtsschutz betroffener Personen. Die Leitung bekennt sich zu dem Organisationsziel und verpflichtet sich zur Förderung der Umsetzung durch die Zurverfügungstellung angemessener Ressourcen.

## Organisatorische Gewährleistung Verzeichnis von Verarbeitungstätigkeiten (Art. 30)

Zweck des Art. 30 DS-GVO ist es, eine Verarbeitung oder Verarbeitungstätigkeit zu erfassen. Abs. 1 S. 1 verpflichtet die Verantwortlichen von Verarbeitungen mit personenbezogenen Daten zum Führen eines Verzeichnisses von Verarbeitungen. Die Anforderungen des Art. 30 DS-GVO zu erfüllen, bedeutet nicht, dass eine Verarbeitung oder Verarbeitungstätigkeit dadurch bereits ausreichend dokumentiert wäre. Das Verzeichnis der Verarbeitungstätigkeit bildet aber die Basis für weitere Aktivitäten, bspw. Erfüllung der Informationspflichten oder Durchführen von Datenschutzfolgenabschätzungen.

Verantwortlicher im Sinne der DS-GVO ist hierbei die Hochschule als juristische Person des öffentlichen Rechts. Ist die Hochschule Auftragsverarbeiter für einen anderen Verantwortlichen muss ein Verzeichnis gemäß Art. 30 Abs. 2 DS-GVO über die Auftragsverarbeitungen geführt werden. Das Verzeichnis der Verarbeitungen dient der internen Kontrolle und muss nur auf Anforderung gegenüber der zuständigen Datenschutzaufsichtsbehörde offengelegt werden. Die dortigen Angaben sind zusammen mit den weiteren notwendigen Dokumentationen zum Nachweis der Einhaltung der Datenschutzgesetze von elementarer Bedeutung und dienen damit der Erfüllung der Rechenschafts­pflicht und zur Gewährleistung der Rechte der Betroffenen gemäß der Artikel 12 bis 22 DS-GVO. Darüber hinaus ist ohne eine entsprechende Dokumentation der angemessene Schutz von Verarbeitungen von personenbezogenen Daten gemäß Art. 32 DS-GVO nicht denkbar.

### Gesetzliche Anforderungen für Verantwortliche an das Verzeichnis von Verarbeitungstätigkeiten

Die gesetzlichen Anforderungen an den Inhalt des Verzeichnisses von Verarbeitungen für Verantwortliche ergeben sich aus Art. 30 Abs. 1 S. 2 DS-GVO:

1. *Name und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie einer oder eines Datenschutzbeauftragten:* Hierbei ist zu beachten, dass mit dem Verantwortlichen die Hochschule als juristische Person gemeint ist. Folglich werden hier die juristische Person mit ihrem gesetzlichen Vertreter und die ladungsfähige Anschrift genannt. Ergänzend sollten für interne Kontrollzwecke auch noch die fachlich verantwortliche Fachabteilung/Verfahrensverantwort­liche (Dezernat/Sachgebiet, Zentrale Einrichtung, …) sowie die fachlichen und technischen Ansprechpartnerinnen oder Ansprechpartner genannt werden. Der Verweis auf den „gemeinsam mit ihm Verantwortlichen“ betrifft den Fall, dass eine gemeinsame Verarbeitung mit einer anderen Stelle (z. B. Kooperation mit einer anderen Hochschule) in der Weise erfolgt, dass beide als Verantwortliche anzusehen sind. Daneben sind Name und Kontaktdaten der oder des behördlichen Datenschutzbeauftragten anzugeben.
2. *Die Zwecke der Verarbeitung:* An dieser Stelle müssen alle Zwecke aufgeführt werden, für die die Daten verarbeitet werden oder werden sollen. Diese Zwecke müssen vollständig durch gesetzliche Rechtsgrundlagen oder Einwilligungen abgedeckt sein.
3. Eine *Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten*. Diese Aufstellung kann aus drei Teilen bestehen:
   1. Hierbei müssen die Personengruppen aufgeführt und unterscheidbar beschrieben werden (z. B. Mitglieder der Hochschule, Beschäftigte, Studierende).
   2. Außerdem müssen die Kategorien personenbezogener Daten mit ihrer Menge von Einzeldaten (z. B. Name, Geschlecht, Alter, Studienstatus, …) aufgeführt werden. Sofern im Einzelfall die Menge an personenbezogenen Einzeldaten fragil ist, sollte auf die Aufzählung der Einzeldaten verzichtet werden, damit die Verfahrensbeschreibung nicht bei jeder Änderung des Datensets angepasst werden muss. Wichtig ist dann die sinnvolle Bezeichnung der Kategorie (z. B. Kontaktdaten für Telefonnummer, Faxnummer, E-Mail-Adresse, Raumnummer). Eine Aufzählung ist in jedem Fall sinnvoll für personenbezogene Daten besonderer Kategorien nach Art. 9 DS-GVO.
   3. Die Kategorien personenbezogener Daten sollten den Kategorien der Personengruppen zugeordnet werden. Diese Zuordnung ist optional, da diese Zuordnung von der Verordnung nicht gefordert wird. Dadurch wird die Verarbeitung aber transparenter dargestellt und lässt sich datenschutzrechtlich einfacher bewerten, wenn beispielsweise im Rahmen der Lehre unterschiedliche Daten von den Studierenden und von den Lehrenden verarbeitet werden. Handelt es sich um eine komplexe Zuordnung, weil von vielen unterschiedlichen Personengruppen unterschiedliche Datenkategorien verarbeitet werden, so bietet sich die Darstellung der Zuordnung in Matrix-Form an. Alternativ können die Personengruppen und Datenkategorien über Nummernkreise verknüpft werden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Datenkat. 1 | Datenkat. 2 | … | Datenkat. n |
| Personengruppe 1 | X |  | … | X |
| Personengruppe 2 | X | X | … |  |
| … | … | … | … | … |
| Personengruppe m |  | X | … | X |

1. *Die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen:* Sofern die personenbezogenen Daten offenbart oder für anderen Zwecke verarbeitet werden, müssen alle Empfänger (ggf. kategorisiert in Empfängerkategorien) angegeben werden, wobei auf die Merkmale einer Empfängerkategorie eingegangen werden sollte. Für jede Kategorie sollten auch die tatsächlichen Empfänger angegeben werden, sofern dies möglich ist. Es kann sich um andere interne Stellen, Auftragsverarbeiter, andere Verantwortliche oder Dritte handeln. An dieser Stelle ist die Angabe der Rechtsgrundlage für die Offenbarung sinnvoll, damit die Überprüfbarkeit durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten und die Aufsichtsbehörde unterstützt wird. Je nach Ausgestaltung der Datenverarbeitung und Offenbarung bietet sich wieder eine Darstellung in Matrix-Form an. Es bietet sich an, in die Zelle sogleich die Rechtsgrundlage einzutragen:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Datenkat. 1 | Datenkat. 2 | … | Datenkat. n |
| Empfängerkat. 1 | § 80 SGB X | § 111 TKG | … |  |
| Empfängerkat. 2 |  | Einwilligung | … | § 87 LBG |
| … | ... | … | … | … |
| Empfängerkat. m | § 8 DSG NRW |  | … | § 8 HG NRW |

1. 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: Sofern die Hochschule beabsichtigt, Daten international zu übermitteln, müssen diese Angaben gemacht werden. Diese Angabe dürfte insbesondere im Kontext von Forschung relevant sein. Sofern für das Drittland kein angemessenes Datenschutzniveau durch die EU-Kommission festgestellt wurde und keine Ausnahme aus Art. 49 Abs. 1 Buchstaben a bis g angewendet werden kann, müssen angemessene Garantien für die Einhaltung des Schutzes personenbezogener Daten aufgeführt werden.
2. Wenn möglich, *die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien:* Verfügt die Hochschule über ein Löschkonzept, dann reicht an dieser Stelle ein Verweis auf dieses Löschkonzept. Andernfalls ist für jede Datenkategorie die Frist oder die Kriterien zur Festlegung der Frist anzugeben. Eine Frist besteht dabei immer aus einem Datum oder Ereignis sowie eines Aufbewahrungszeitraums. Sofern möglich sollten auch die gesetzlichen Grundlagen oder andere Gründe für die Festlegung des Aufbewahrungszeitraums angegeben werden.
3. Wenn möglich, *eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1:* Hierbei kann ein Verweis auf ein Informationssicherheitskonzept für allgemeine Maßnahmen genügen. Sollten für die konkrete Verarbeitung spezielle oder weitere Maßnahmen erforderlich sein, so sollten diese zusätzlich angegeben werden.

### Über Art. 30 Abs. 1 DS-GVO hinausgehende Angaben

Neben den in Art. 30 Abs. 1 DS-GVO genannten Angaben ist es sinnvoll, das Verzeichnis der Verarbeitungen um weitere Angaben zu ergänzen. Das Ziel ist eine zentrale Dokumentation einer Verarbeitung, mit der sich neben den Anforderungen des Art. 30 Abs. 1 DS-GVO auch die Rechenschaftspflicht und die Erfüllung der Informationspflicht und der Betroffenenrechte realisieren lässt. Vergleicht man die Anforderungen an Informationen nach Art. 13 und 14 DS-GVO mit den nach Art. 30 Abs. 1 DS-GVO erforderlichen Angaben wird deutlich, dass über die Pflichtangaben hinausgehende Informationen wie z. B. die Rechtsgrundlage der Verarbeitung erforderlich sind. Dies soll jedoch in einer leicht abtrennbaren Rubrik erfolgen, da sich die Pflicht zur Offenlegung des Verzeichnisses gegenüber der Datenschutzaufsichtsbehörde nach Art. 30 Abs. 4 DS-GVO nur auf die Pflichtangaben nach Art. 30 Abs. 1 DS-GVO erstreckt.

### Gesetzliche Anforderungen für Auftragsverarbeiter an das Verzeichnis von Verarbeitungstätigkeiten

Verarbeitet die Hochschule Daten im Interesse eines anderen Verantwortlichen und unterliegt sie dabei dessen Weisungen, muss sie diese Verarbeitungen nach den Anforderungen von Art. 30 Abs. 2 DS-GVO dokumentieren. Es handelt sich dabei um die folgenden Angaben:

1. *Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines Datenschutzbeauftragten oder einer Datenschutzbeauftragten:* Hierbei ist der Auftraggeber für die Auftragsverarbeitung zu nennen. Dies muss nicht der Verantwortliche sein, sondern kann ein Auftragsverarbeiter oder Unterauftragsverarbeiter in einer Kette von Auftragsverarbeitungsverhältnissen sein. Es muss hierbei die juristische Person mit gesetzlichem Vertreter und einer ladungsfähigen Anschrift angegeben werden. Für interne Kontrollzwecke sollen die internen fachlichen und ggf. technischen Ansprechpartner aufgeführt werden.
2. *Die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden:* An dieser Stelle muss angegeben werden, welche (Teil-)Verarbeitung für welchen Auftraggeber durchgeführt wird. Ein Auftragsverarbeiter wird zum Verantwortlichen für die Unterauftragsverhältnisse, daher kann an dieser Stelle von Verantwortlichen oder Auftraggebern gesprochen werden. Sollten mehrere Teilverarbeitungen mit mehreren Verantwortlichen verknüpft sein, wobei nicht jeder Verantwortliche die gleiche Gruppe von Teilverarbeitungen beauftragt hat, dann bietet sich die Darstellung in Matrixform an.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Teilverarbeitung 1 | Teilverarbeitung 2 | … | Teilverarbeitung n |
| Auftraggeber 1 | X |  | … | X |
| Auftraggeber 2 | X | X | … |  |
| … | … | … | ... | … |
| Auftraggeber m |  | X | … | X |

1. Siehe Punkt e) für Verantwortliche
2. Siehe Punkt g) für Verantwortliche

### Abgrenzung zu beschreibender Verarbeitungen

Der Begriff der Verarbeitung ist in Art. 4 Abs. 2 DS-GVO definiert. Unter Verarbeiten sind subsumiert:

„das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung [also Datenübertragung im allgemeinsten Sinne], Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“

Eine Verarbeitung ist eine wiederholbare Menge von Datenverarbeitungen mit personenbezogenen Daten, die zu einem bestimmten Zweck durchgeführt werden. Dies können mehrere einzelne Verarbeitungen sein, die räumlich oder fachlich getrennt durchgeführt werden. Das verbindende Element ist der gleiche Zweck, zu dem die Datenverarbeitung durchgeführt wird, und der einer Verarbeitung zugrunde liegt. Eine Software kann so u. U. auch für verschiedene Verarbeitungen eingesetzt werden. Aus diesem Grund kann die Verarbeitung somit nicht von einem bestimmten IT-Verfahren abgeleitet werden. Vielmehr muss vom jeweiligen Zweck ausgegangen werden. Am Zweck einer Verarbeitung knüpft auch die rechtliche Erlaubnis an, da gesetzliche Erlaubnisnormen und Einwilligungen immer von einem Verarbeitungszweck ausgehen müssen. Nicht beschrieben werden müssen Verarbeitungen, die ausschließlich nichtautomatisiert erfolgen und dabei weder in einem Dateisystem gespeichert sind oder gespeichert werden sollen (siehe Art. 2 Abs. 1 DS-GVO), wie z. B. ein Karteikartenkasten.

### Zuständigkeit/Verantwortlichkeit

Die Verantwortlichkeit liegt bei der Hochschule als juristische Person, so dass die Hochschulleitung die Gesamtverantwortung für die Erstellung und weitere Führung des Verzeichnisses von Verarbeitungen trägt. Das Präsidium der Hochschule hat mit Beschluss vom <TT.MM.JJJJ> die Zuständigkeit für die Erstellung, Meldung von Veränderungen und Führung des Verzeichnisses der Verarbeitungstätigkeiten wie folgt geregelt:

* Die Beschreibungen werden durch die jeweiligen fachlich verantwortlichen Personen einer Verarbeitung erstellt. Fachlich verantwortlich ist diejenige Person, die die Verarbeitung beherrscht, indem sie über das Ob und Wie der Verarbeitung entscheidet. Ausschlaggebend ist die fachliche Entscheidungsmöglichkeit unabhängig von der technischen Beherrschung.
  + Ist eine Organisationseinheit verantwortlich, liegt die Verantwortung bei der Leitung der Organisationseinheit, die diese an eine geeignete Mitarbeiterin / einen geeigneten Mitarbeiter delegieren kann.
  + Die Verantwortung für die Verwaltungseinheiten obliegt der Leitung der jeweiligen Organisationseinheit.
  + Ist eine Fakultät verantwortlich, liegt die Verantwortung beim jeweiligen Dekanat.
  + Ist ein Institut verantwortlich, liegt die Verantwortung bei der Institutsleitung.
  + Bei der Verarbeitung im Rahmen von Forschungsvorhaben ist die jeweilige Projektleitung verantwortlich.
* Der oder dem Datenschutzbeauftragten obliegt nach Art. 39 Abs. 1 lit. b DS-GVO die interne Kontrollpflicht, ob die gesetzlichen Anforderungen an die Dokumentation von Verarbeitungstätigkeiten eingehalten werden. Es wird somit durch die Hochschulleitung entschieden, dass sämtliche Verarbeitungen und Veränderungen an bestehenden Verarbeitungen an die behördliche Datenschutzbeauftragte / den behördlichen Datenschutzbeauftragten gemeldet werden und damit alle Verarbeitungen dort gesammelt werden. (Alternative Gestaltung: Sämtliche Verarbeitungen und Veränderungen an bestehenden Verarbeitungen werden an die der Hochschulleitung direkt unterstellte Stabsstelle Datenschutz gemeldet. Die Stabsstelle Datenschutz führt das Verzeichnis der Verarbeitungen an der Hochschule und gewährleistet, dass der/die behördliche Datenschutzbeauftragte zu Kontrollzwecken jederzeit Zugriff erhält.)

### Umsetzung

Die Meldung eines Verfahrens muss vor der ersten Verarbeitung personenbezogener Daten erfolgen und die Aktualisierung bereits erfasster Verfahrensbeschreibungen vor Änderung des Verfahrens im Produktivbetrieb. Erfolgt keine Änderungsmeldung durch den Verfahrensverantwortlichen, muss dieser im Abstand von jeweils zwei Jahren die Vollständigkeit und Korrektheit bestätigen. Wird eine Verarbeitung eingestellt, ist dies ebenfalls an den behördlichen Datenschutzbeauftragten oder die behördliche Datenschutzbeauftragte zu melden. Die operative Umsetzung soll folgendermaßen erfolgen:

1. **Fragebogen zur Ersterfassung:** Für eine erleichterte Erfassung von Verarbeitungen wird ein Fragebogen für die Ersterfassung von Verarbeitungen zur Verfügung gestellt. Dieser fragt die nach Art. 30 DS-GVO erforderlichen Informationen so ab, dass auch nicht im Datenschutz vorgebildete Personen diesen in einem vertretbaren Zeitrahmen (ca. 60 Minuten) beantworten können. Über diese Mindestinformationen hinaus enthält der Fragebogen einige ergänzende Fragen, die Anhaltspunkte für einen möglicherweise erhöhten Schutzbedarf sammeln sollen. Derzeit existiert der Fragebogen nur in Form einer Word-Datei, so dass bei einer Übertragung in das elektronische Verzeichnis ein zusätzlicher Kopier- und Ordnungsaufwand entsteht.
2. **Unterstützung durch Datenschutzkoordinatorinnen / -koordinatoren:** Für jeden fachlichen Bereich erfolgt die Unterstützung durch Datenschutzkoordinatorinnen / -koordinatoren. Diese sind entsprechend geschult, um den Verfahrensverantwortlichen Fragen rund um das Ausfüllen des Erfassungsbogens beantworten zu können. Die Datenschutzkoordinatorinnen / -koordinatoren werten die Antworten aus und stellen gegebenenfalls Rückfragen, die zu einer Vervollständigung oder weiteren Klärung führen. Außerdem können gleichartige oder ähnliche Verarbeitungen in einem Verfahren integriert und zusammen dokumentiert werden, um doppelte Dokumentation zu vermeiden. Sollte sich aufgrund der Art der Verarbeitung, den verarbeiteten Datenfeldern oder aus einem anderen Grund weiterer Untersuchungs- oder Dokumentationsbedarf ergeben, so unterstützt der Datenschutzkoordinator bei der Festlegung des erforderlichen Dokumentationsumfangs und der Erhebung weiterer Daten zusammen mit dem Verfahrensverantwortlichen. Die Verantwortung für die ausführlichere Dokumentation verbleibt bei dem Verfahrensverantwortlichen. Die Datenschutzkoordinatorinnen / -koordinatoren sind in der Lage zu erkennen, ob gegebenenfalls ein erhöhter Schutzbedarf bestehen könnte, was dann jedoch im Detail durch den behördlichen Datenschutzbeauftragten oder die behördliche Datenschutzbeauftragte überprüft werden muss (siehe bei Datenschutzfolgeabschätzung). Für die Durchführung der Meldung bei dem oder der behördlichen Datenschutzbeauftragten bleibt die / der Verfahrensverantwortliche verantwortlich.
3. **Elektronisches Verzeichnis:** Da das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 3 DS-GVO elektronisch geführt werden kann, wird ein zentralisiertes System zur Speicherung der Verfahrensbeschreibungen und Bereitstellung des Verzeichnisses der Verarbeitungstätigkeiten eingesetzt. Die Kontrolle über dieses elektronische Verzeichnis übt der oder die behördliche Datenschutzbeauftragte (Alternativ: die Stabsstelle Datenschutz) aus, wobei die Inhalte (also die Verfahrensbeschreibungen) durch die Verfahrensverantwortlichen und Datenschutzkoordinatorinnen/-ko­or­dina­toren eingepflegt werden müssen. Das System sollte eine Ausgabe als Datei unterstützen, damit der jeweils aktuelle Stand der Dokumentation auf Anforderung an die zuständige Datenschutzaufsichtsbehörde herausgegeben werden kann. Es müssen ein Zugriffsschutz sowie eine Versionierung für das Verzeichnis eingerichtet werden.

### Aufarbeitung des bestehenden Rückstands

Momentan sind nicht alle Verarbeitungen vollständig dokumentiert. Die Verpflichtung zur Erstellung eines Verzeichnisses für Verarbeitungen umfasst auch die Bestandsverfahren und beschränkt sich nicht auf neue Verfahren ab dem 25.05.2018. Für die Nachholung noch fehlender Verzeichnisse von Verarbeitungen muss eine Übergangszeit eingeplant werden. Um einen möglichst schnellen Gesamtüberblick über die eingesetzten Verarbeitungen mit personenbezogenen Daten zu bekommen, soll wie folgt vorgegangen werden:

1. Es findet zunächst nur eine Erfassung anhand des Fragebogens zur Ersterfassung statt. Dies gilt auch für die Nacherfassung von Bestandsverfahren. Die möglichst vollständigen Ergebnisse werden in das elektronische Verzeichnis übertragen. Somit ist gewährleistet, dass zumindest die Pflichtangaben aus Art. 30 DS-GVO vorliegen.
2. Verarbeitungen in Word- oder Excel-Dateien werden grundsätzlich nicht erfasst. Eine Ausnahme bilden Listen bei denen außer Name, Geburtsdatum, Geburtsort und Kontaktdaten noch weitere Daten verarbeitet werden.
3. In der Folgezeit wird je nach möglichem Schutzbedarf der Verarbeitung die Dokumentation erweitert.

**Handreichungen:**

* Fragebogen zur Erstabfrage bei den Verantwortlichen
* Vorlage Verzeichnis Verarbeitungen Verantwortlicher
* Vorlage Verzeichnis Verarbeitungen Auftragsverarbeiter
* Ausfüllhinwiese Verzeichnis Verarbeitungen

## Organisatorische Gewährleistung der Umsetzung verarbeitungsbezogener Anforderungen (Art. 5 Abs. 1)

Die Hochschule kann die Umsetzung verarbeitungsbezogener Anforderungen nur gewährleisten, wenn die diesbezüglichen Verantwortlichkeiten geklärt sind. Gesetzlich verantwortlich ist der Verantwortliche für die jeweilige Verarbeitung. Damit ist die Organisation als solche gemeint, in deren Interesse die Verarbeitung stattfindet und somit die Hochschule als juristische Person. Die Hochschule als juristische Person ist als solche aber nicht selbst handlungsfähig, sondern nur über die Hochschulleitung als gesetzlichen Vertreter. Da aber die Hochschulleitung nicht die verarbeitungsbezogenen Anforderungen aller stattfindenden Verarbeitungen selbst umsetzen kann, muss eine sinnvolle Aufgabenteilung innerhalb der Hochschule erfolgen, die nachweislich die Einhaltung der verarbeitungsbezogenen Anforderungen gewährleistet:

### Hochschulleitung

Die Hochschulleitung trägt die Gesamtverantwortung für die Einhaltung der organisatorischen und verarbeitungsbezogenen gesetzlichen Anforderungen bei der Verarbeitung von personenbezogenen Daten. Dies beinhaltet:

1. Die Gewährleistung der Umsetzung der gesetzlichen Anforderungen zum Datenschutz (Compliance) mittels
   1. Satzungen/Ordnungen, Anweisungen und Policies zur Verarbeitung von personenbezogenen Daten
   2. Bereitstellung der erforderlichen finanziellen, sachlichen und personellen Ressourcen
2. Umsetzung der Nachweispflichten (Accountability)
3. Sicherstellung einer ordnungsgemäßen Überwachung datenschutzrelevanter Prozesse durch die Installation ausreichender Kontrollmechanismen. Dies kann z. B. durch einen zentralen Datenschutzkoordinator mit entsprechenden Befugnissen erfolgen.
4. Errichtung eines Systems zur kontinuierlichen Verbesserung (Datenschutz-Management) mit entsprechend verbindlichen Vorgaben an alle verantwortlichen Personen, die mit der Verarbeitung von personenbezogenen Daten befasst sind.

### Stabsstelle Datenschutz

Die Stabsstelle Datenschutz koordiniert mit entsprechendem juristischem und technischem Sachverstand für die Hochschulleitung die hochschulweite Umsetzung der Anforderungen. Sie ist die zentrale Kompetenzstelle und übernimmt die Prüfung und Umsetzung bei Verarbeitungen, die durch die Verantwortlichen der Verarbeitung auch mit Unterstützung von Datenschutz-Koordinatoren nicht bewältigt werden können, weil spezielle juristische oder technische Kenntnisse erforderlich sind. Aufgaben der Stabsstelle Datenschutz:

1. Rechtliche Vorbereitung von Satzungen/Ordnungen, Anweisungen und Policies
2. Pflege von Musterverträgen, Unterstützung von Verantwortlichen bei besonderen rechtlichen Konstellationen (insb. Auftragsverarbeitung AV und Drittstaatenübermittlung)
3. Führung des Verzeichnisses der Verarbeitungen
4. Verbindliche Prüfung ob eine DSFA erforderlich ist
5. Durchführung DSFA mit dem Verantwortlichen mit Entscheidungsbefugnis ergänzender technischer und organisatorischer Maßnahmen gegenüber der Projektmanagerin/dem Projektmanager. Auf Anfrage unterstützt der/die behördliche Datenschutzbeauftragte die Durchführung der DSFA. Unabhängig davon besteht ein Kontrollrecht des/der behördlichen Datenschutzbeauftragten.
6. Die Stabsstelle berichtet direkt an die Hochschulleitung

### Verfahrensverantwortlicher

Die Umsetzung der datenschutzrechtlichen Anforderungen obliegt den für die jeweilige Verarbeitung zuständigen Verfahrensverantwortlichen. Sie beherrschen die Verarbeitung/das Verfahren, kennen die fachlichen Anforderungen und treffen alle wesentlichen Entscheidungen (über Zwecke und Mittel) bezüglich der Verarbeitung. Ohne eine explizite Nennung einer für die Verarbeitung verantwortlichen Person, ist die jeweilige Organisationseinheit bzw. der jeweilige Lehrstuhl und personell deren bzw. dessen Leitung verantwortlich. Die Verantwortung umfasst insbesondere folgendes:

* Beschreibung der Verarbeitung für das Verzeichnis der Verarbeitungen nach den Anforderungen von Art. 30 DS-GVO plus der zusätzlich für die Erfüllung der Rechenschaftspflicht erforderlichen Angaben und Meldung an die Stabsstelle Datenschutz.
* Meldung aller Änderungen an die Stabsstelle Datenschutz
* Klärung der Rechtmäßigkeit der Verarbeitung bzw. deren Sicherstellung durch Einwilligungen bzw. vertragliche Vereinbarungen bei Einbeziehung Dritter
* Umsetzung der Informationspflicht in Bezug auf die jeweilige Verarbeitung
* Durchführung einer Schwellwertanalyse (Schutzbedarfsanalyse) bzw. Veranlassung einer verbindlichen Prüfung durch die Stabsstelle Datenschutz
* Gewährleistung der Sicherheit der Verarbeitung und Einhaltung zusätzlicher Anforderungen aus der DSFA bei erhöhtem Schutzbedarf der Verarbeitung; Umsetzung geeigneter technischer, organisatorischer und personeller Maßnahmen
* Umsetzung der Betroffenenrechte (insb. Auskunft und Löschung) bzw. Unterstützung der / des Datenschutzbeauftragten der Hochschule bei der Realisierung der Betroffenenrechte
* Unverzügliche Meldung von Vorfällen mit Bezug zu personenbezogenen Daten an die Stabsstelle Datenschutz
* Geordnete Dokumentation der Verarbeitung, damit die Hochschule ihrer Rechenschaftspflicht jederzeit auf Anforderung nachkommen kann

### Beschäftigte

Ohne die Mitwirkung und die Umsicht sämtlicher Beschäftigter, ist die Einhaltung der Vorgaben zum Datenschutz kaum vorstellbar. Folgende Aufgaben kommen den Beschäftigten zu:

* Keine Verarbeitung dienstlich erlangter Daten zu privaten Zwecken. Ansonsten besteht die Gefahr einer Ordnungswidrigkeit oder gar einer Straftat.
* Wahrnehmung der Schulungs- und Informationsangebote um sich mit den gesetzlichen und internen Regelungen zum Datenschutz vertraut zu machen.
* Meldung an die Vorgesetzte / den Vorgesetzten bei Vorfällen oder in Zweifelsfällen, der wiederum die Datenschutzbeauftragte / den Datenschutzbeauftragten der Hochschule informiert.

### Datenschutz- und Informationssicherheits-Koordinatorinnen / -koordinatoren

Zur Unterstützung von Verantwortlichen und Beschäftigten sollen in den Organisationseinheiten Datenschutz- und Informationssicherheitskoordinatorinnen bzw. -koordinatoren etabliert werden. Dies sind Personen denen die fachlichen Anforderungen und die Aufbau- und Ablauforganisation aus der jeweiligen Organisationseinheit bekannt sind und die über Fachkenntnisse in Informationssicherheit und/oder Datenschutz verfügen oder zumindest ein Interesse hieran mitbringen. Diese Koordinatorinnen und Koordinatoren werden so geschult und mit Arbeitsvorlagen vertraut gemacht, dass diese die Verantwortlichen und die Beschäftigten in ihrer jeweiligen Organisationseinheit unterstützen können. Folgende Aufgaben sind hierbei vorgesehen:

* Unterstützung der Verantwortlichen bei Einführung und Anpassung von Verarbeitungen, wobei die Verantwortlichkeit bei den Verantwortlichen verbleibt. Bei speziellen Problematiken wird die Stabsstelle Datenschutz mit eingebunden.
* Ansprechpartner der Beschäftigten in der Organisationseinheit bei Fragen zu Sicherheit und Datenschutz
* Informierte Ansprechpersonen für die /den bDSB, die Stabsstelle Datenschutz und die Informationssicherheitsbeauftragte / den Informationssicherheitsbeauftragten
* Regelmäßige Teilnahme am Lenkungskreis Informationssicherheit und Datenschutz mit anderen Koordinatorinnen und Koordinatorenen, bDSB und Informationssicherheitsbeauftragter/Informationssicherheitsbeauftragten zum gegenseitigen Austausch und Erhalt des Know-how.

### Behördliche Datenschutzbeauftragte / Behördlicher Datenschutzbeauftragter

Die bzw. der behördliche Datenschutzbeauftragte (bDSB) überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz und Zuständigkeiten sowie die Sensibilisierung der Beschäftigten durch Schulungen. Im Einzelnen umfasst dies die folgenden Aufgaben:

* Überwachung der Umsetzung der gesetzlichen Anforderungen an den Datenschutz in der Hochschule.
* Beratung der Hochschulleitung und der weiteren für die Umsetzung des Datenschutzes verantwortlichen Personen (Stabsstelle Datenschutz, Verantwortliche, Beschäftigte)
* Beratung der Datenschutz- und Informationssicherheitskoordinatorinnen und -koordina­torenbei deren Aufgabenerfüllung.
* Neben dem Verantwortlichen Anlaufstelle für betroffene Personen.
* Ansprechpartner für die zuständige Datenschutzaufsichtsbehörde

### Informationssicherheitsbeauftragte / Informationssicherheitsbeauftragter

Die bzw. der Informationssicherheitsbeauftragte ist die Kompetenzstelle für Informationssicherheit innerhalb der Hochschule. Sie / er übernimmt die die folgenden Aufgaben:

* Beratung der Hochschulleitung, der Stabsstelle Datenschutz, der Verantwortlichen, der Beschäftigten, den Datenschutzkoordinatorinnen und -koordinatoren sowie der / des bDSB bei Fragen der Informationssicherheit.
* Regelmäßiger und anlassbezogener Austausch mit der / dem bDSB zu Maßnahmen der Informationssicherheit und der Sicherheit der Verarbeitung personenbezogener Daten und zu datenschutzrelevanten Sicherheitsvorfällen. Bei Konflikten zwischen Zielen der Informationssicherheit und des Datenschutzes wirken bDSB und Informationssicherheitsbeauftragte/Informationssicherheitsbeauftragter auf eine Lösung hin, die beiden Aspekten angemessen Rechnung trägt.

## Effektive Datenschutzkontrolle (Art. 37 -39)

Die Hochschule benennt einen behördlichen Datenschutzbeauftragten oder eine behördliche Datenschutzbeauftragte (bDSB) gemäß Art. 37 Abs. 1 lit. a DS-GVO unter Berücksichtigung der gesetzlichen Anforderungen an die Stelle und die ausführende Person. Dazu gehört auch, der Person keine weiteren Aufgaben zu geben, die zu einem Interessenskonflikt führen könnten, insbesondere darf der oder die Datenschutzbeauftragte keine Führungsposition mit Verfahrensverantwortung einnehmen und keine Verfahren verantworten. Zudem darf der Datenschutzbeauftragte nicht zugleich der Informationssicherheitsbeauftragte sein, damit im Falle eines Konflikts zwischen Informationssicherheitsinteressen der Organisation mit Grundrechtsinteressen der betroffenen Person eine argumentative Auseinandersetzung ermöglicht wird und nicht die subjektive Ansicht einer Person entscheidet.

Die Hochschulleitung verpflichtet sich, der oder dem Datenschutzbeauftragten die erforderlichen Ressourcen in zeitlichen und materiellen Dimensionen zur Wahrnehmung der gesetzlichen Aufgaben bereitzustellen. Dazu gehört die Freistellung von anderen Aufgaben sofern dies zur Erfüllung der Aufgaben als Datenschutzbeauftragte / Datenschutzbeauftragter erforderlich ist und die Möglichkeit zum Erhalt der Fachkunde durch Fortbildungsmaßnahmen sowie zum Austausch mit Datenschutzbeauftragten anderer Hochschulen.

Der oder die Datenschutzbeauftragte wird beratend in die Geschäftsprozesse und Gestaltung der IT-Stra­tegie einbezogen. Dazu gehört auch, dass die Verantwortung von anderen Personen übernommen wird und Entscheidungen durch andere Personen getroffen werden, der Rat der oder des Datenschutzbeauftragten aber beachtet werden muss. Die Hochschulleitung stellt sicher, dass die oder der Datenschutzbeauftragte weisungsfrei mit Bezug zur Verarbeitung personenbezogener Daten agieren kann.

Die oder der Datenschutzbeauftragte arbeitet eng mit der oder dem Informationssicherheitsbeauftragten der Hochschule zusammen, um die datenschutzrechtlichen Anforderungen auch bei Maßnahmen im Bereich der Informationssicherheit und die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Die oder der Datenschutzbeauftragte wird bei der Zuweisung von Berechtigungen gehört, insbesondere wenn Rollen oder Personen Berechtigungen aus mehreren Arbeitsbereichen zugeordnet werden sollen.

Der oder dem Datenschutzbeauftragten obliegt die Kontrolle und Überwachung der Einhaltung der datenschutzbezogenen Rechtsnormen gemäß Art. 39 Abs. 1 lit. b DS-GVO. Sie bzw. er führt die erforderlichen Kontrollen und Überprüfungen der Prüfungen durch den Verantwortlichen durch. Die Hochschulleitung stellt sicher, dass der oder dem Datenschutzbeauftragten die zur Aufgabenerfüllung erforderlichen Zugänge und Unterlagen unverzüglich zur Verfügung gestellt werden. Dies betrifft insbesondere, aber nicht ausschließlich, Dokumentationen zu

* dem Verzeichnis der Verarbeitungstätigkeiten,
* der Gewährleistung der Betroffenenrechte und Einhaltung der Informationspflichten,
* der Ergebnisse von Datenschutzfolgenabschätzungen,
* Datenpannen und die Meldeprotokolle gegenüber Aufsichtsbehörde, Verantwortlichen und betroffenen Personen,
* Dokumentation zur Einhaltung des Löschkonzepts,
* den von dem Verantwortlichen eigenständig durchgeführten Prüfungen vor Einführung oder Änderung von Verarbeitungen (Datenschutzfolgenabschätzungen) .

## Angemessene Maßnahmen für die Sicherheit personenbezogener Daten (Art. 32)

Mit Blick auf die Sicherheit der Verarbeitung von personenbezogenen Daten verlangt Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Bestimmung des angemessenen Niveaus im Einzelfall sind zu berücksichtigen:

* Stand der Technik
* Implementierungskosten (Wirtschaftlichkeit)
* Art, Umfang, Umstände und Zwecke der Verarbeitung
* Eintrittswahrscheinlichkeiten
* Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

### Informationssicherheit und Art. 32 DS-GVO

In Bezug auf die Gewährleistungsziele Vertraulichkeit, Verfügbarkeit und Integrität von Informationen gibt es weitgehende Parallelen zwischen der Informationssicherheit und dem Datenschutzziel der Gewährleistung der Sicherheit der Verarbeitung von personenbezogenen Daten. Der Unterschied ergibt sich aus dem jeweiligen Fokus, der bei der Informationssicherheit auf mögliche Folgen für die Organisation gerichtet ist, während der Datenschutz den Betroffenen und Auswirkungen auf dessen Grundrechte im Blick hat. Entsprechend werden für die Gewährleistungsziele Vertraulichkeit, Verfügbarkeit und Integrität gemeinsame Maßnahmen verfolgt, die auf ausreichende Berücksichtigung des Datenschutzes überprüft werden. Bei einem Konflikt zwischen Informationssicherheit und Datenschutz muss eine Lösung gefunden werden, die sowohl den Interessen der Organisation als auch den Grundrechten der Betroffenen angemessen Rechnung trägt. Ist der Schutzbedarf aus Sicht des Datenschutzes höher als für die Informationssicherheit, muss in Bezug auf das jeweilige Gewährleistungsziel eine Maßnahme für einen hohen Schutzbedarf ausgewählt werden. Gleiches gilt umgekehrt, wenn der Schutzbedarf aus Sicht der Informationssicherheit höher ist als beim Datenschutz.

Die genannten Parallelen erschöpfen sich auf die Schutz- und Gewährleistungsziele Vertraulichkeit, Verfügbarkeit und Integrität. Die weiteren Gewährleistungsziele des Datenschutzes (Datensparsamkeit, Transparenz, Nichtverkettbarkeit, Intervenierbarkeit) müssen separat für den Datenschutz geprüft und mit entsprechenden technischen und organisatorischen Maßnahmen unterlegt werden.

### Vorrang technischer Maßnahmen

Bei der Auswahl von Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung von personenbezogenen Daten haben wirksame technische Maßnahmen Vorrang vor organisatorischen Maßnahmen. Organisatorische Maßnahmen ergänzen technische Maßnahmen dort, wo dies zu einer Erhöhung der Wirksamkeit des Schutzes beiträgt. Kommen technische Maßnahmen nicht in Betracht oder reichen diese nicht aus, muss die Sicherheit durch organisatorische Maßnahmen (Arbeits- oder Dienstanweisungen, Anordnungen) gewährleistet werden.

### Stand der Technik

Der Stand der Technik ist ein wesentlicher Maßstab dafür, ob angemessene Maßnahmen zum Schutz der Verarbeitung personenbezogener Daten ergriffen werden. Es findet sich im Gesetz keine Definition für den Begriff „Stand der Technik“. Die einzige offizielle Erläuterung des Begriffs findet sich in der Begründung zu § 8a BSI-Gesetz, in dem im Zusammenhang mit der Informationssicherheit ebenfalls auf den Stand der Technik als Maßstab abgestellt wird. Der Stand der Technik ist demnach der „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt“. Für die Auswahl konkreter Maßnahmen lässt sich hieraus nichts Konkretes ableiten. Sicherheit im Sinne einer gesetzlichen Vermutung der Einhaltung des Stands der Technik bieten lediglich die Zertifizierung nach Art. 42 DS-GVO und die Einhaltung gemeinsamer genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO. Entsprechende von den Aufsichtsbehörden genehmigte Zertifizierungsverfahren und Verhaltensregeln existieren [Stand Ende 2018] noch nicht. Als einzige praktikable Möglichkeit mit Blick auf die Auswahl von Einzelmaßnahmen verbleibt die Möglichkeit des Rückgriffs auf die Maßnahmenkataloge von anerkannten Standards zur Informationssicherheit (ISO 2700x, IT-Grundschutz). Ein Maßnahmenkatalog zum Standard-Datenschutzmodell (SDM) existiert derzeit noch nicht vollständig, so dass nur der Rückgriff auf die Kataloge zur Informationssicherheit verbleibt. Erste und wichtige Maßnahmen zum SDM-Katalog sind bereits vom Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ veröffentlicht worden. Aufgrund der breiten Anerkennung der genannten Standards und ihrer regelmäßigen Aktualisierung, ist die Orientierung hieran derzeit der sicherste Weg zur nachweisbaren Einhaltung der gesetzlichen Vorgaben. Die Maßnahmen aus der Informationssicherheit müssen jedoch darauf überprüft werden, ob sie auch den Anforderungen des Schutzes der Grundrechte der betroffenen Personen gerecht werden.

### Basis-Sicherheit

Ziel ist eine zwischen Informationssicherheit und Datenschutz abgestimmte Sicherheitsstrategie zur Gewährleistung einer Grundsicherheit in der Organi­sation, die den normalen Schutzbedarf von Datenverarbeitungen sowohl aus Sicht der Informationssicherheit als auch aus Sicht des Datenschutzes abdeckt. Hierfür ist die Erstellung eines gemeinsamen Sicherheitskonzeptes und dessen dokumentierte Umsetzung erforderlich. Aufgrund der heterogenen IT-Struktur an der Hochschule ist dies realistischerweise nur für die zentralen IT-Dienste durch das Rechenzentrum möglich. Dies hat aber immer noch den erheblichen Vorteil, dass bei Verarbeitungen die auf die zentrale IT zugreifen und bei denen nur der normale Schutzbedarf vorliegt, bei den technischen und organisatorischen Maßnahmen auf das Sicherheitskonzept verwiesen werden kann. Bei einem erhöhten Schutzbedarf können ausgehend von der Basis-Sicherheit zusätzliche Sicherheitsmaßnahmen ergriffen werden, die dem erhöhten Schutzbedarf im Einzelfall gerecht werden.

**Erforderliche Dokumente:**

* Gemeinsames Sicherheitskonzept zur Gewährleistung einer Basis-Sicherheit für die zentral zur Verfügung gestellten IT-Dienste.

### Schwellwertanalyse und Schutzbedarfsfeststellung

Für die Feststellung ob ein hohes Risiko besteht, muss eine Schwellwertanalyse (Datenschutz) bzw. Schutzbedarfsfeststellung (Informationssicherheit) durchgeführt werden. Eine für Informationssicherheit und Datenschutz parallele Schwellwertanalyse bzw. Schutzbedarfsfeststellung kann für die Gewährleistungs- bzw. Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität erfolgen. Aufgrund des unterschiedlichen Fokus lässt sich die Prüfung aber nicht vereinheitlichen, sondern muss parallel für den Datenschutz und die Informationssicherheit erfolgen.

Für die darüber hinaus gehenden weiteren Gewährleistungsziele des Datenschutzes (Datensparsamkeit, Transparenz, Nichtverkettbarkeit, Intervenierbarkeit) muss eine gesonderte Prüfung nur für den Datenschutz erfolgen.

Trotz der separaten Prüfung wird eine gemeinsame Abbildung von Datenschutz und Informationssicherheit angestrebt, weil auch die reinen Gewährleistungsziele des Datenschutzes einer technischen Umsetzung bedürfen. So bedarf es z. B. zur Umsetzung des Gewährleistungsziels der Nichtverkettbarkeit regelmäßig auch technischer Maßnahmen. Somit ist ein Gesamtbild aus den Anforderungen aus Informationssicherheit und Datenschutz hilfreich.

Besteht ein hohes Risiko, muss eine Risikoanalyse / Datenschutzfolgeabschätzung (DSFA) erfolgen.

**Erforderliche Dokumente:**

* Dokument mit den Prüfkriterien für die Schwellwertanalyse (Datenschutz) und Schutzbedarfsanalyse (Informationssicherheit). Die Anforderungen für die Schwellwertanalyse werden nicht parallel, sondern in einem separaten Anhang geprüft. Die Prüfung beim Datenschutz umfasst nur die Kriterien für einen hohen Schutzbedarf, weil ein normaler Schutzbedarf bei Vorliegen personenbezogener Daten stets gegeben ist.
* Prüfung der Abbildung der Anforderungen in einem unterstützenden Tool, wie z. B. dem PIA-Tool der französischen Datenschutzaufsichtsbehörde CNIL.

### Risikoanalyse/Datenschutzfolgeabschätzung (DSFA)

#### Hohes Risiko nur für die Informationssicherheit

Ergibt die Schwellwert-/Schutzbedarfsanalyse nur für die Informationssicherheit ein hohes Risiko, erfolgt die Risikoanalyse nur aus Sicht der Informationssicherheit. Auf Basis der Ergebnisse werden zusätzliche Sicherheitsmaßnahmen modelliert. Eine Akzeptanz von Risiken ist für den Bereich der Informationssicherheit möglich.

#### Hohes Risiko sowohl für die Informationssicherheit als auch für den Datenschutz

Ergibt sich sowohl für die Informationssicherheit als auch für den Datenschutz ein hohes Risiko, erfolgt eine gemeinsame Risikoanalyse/DSFA, wobei bei der Informationssicherheit die Risiken für die Organisation und beim Datenschutz die Risiken für die betroffenen Personen betrachtet werden. Stehen die jeweiligen Risiken fest, können zusätzliche Maßnahmen zum Ausschluss oder der Verminderung der hohen Risiken festgelegt werden. Hierbei ist zu beachten, dass die Akzeptanz von Risiken im Datenschutz keine Lösungsoption ist. Kann ein hohes Risiko für die Grundrechte der Betroffenen nicht wirksam eingedämmt werden, muss die zuständige Datenschutzaufsichtsbehörde konsultiert werden.

#### Hohes Risiko nur für den Datenschutz

Ergibt sich nur aus dem Datenschutz ein hohes Risiko, ist eine Datenschutzfolgeabschätzung (siehe unten bei Datenschutzfolgeabschätzung) durchzuführen. Mit Blick auf die Gewährleistungsziele Vertraulichkeit, Verfügbarkeit und Integrität kann auf den gemeinsamen Prüfrahmen mit der Informationssicherheit zurückgegriffen werden, wobei der spezifischen Schutzperspektive des Datenschutzes (Maßnahmen des Vertraulichkeitsschutzes für Betroffene) Rechnung zu tragen ist. Im Gegensatz zur Informationssicherheit ist die Akzeptanz von Risiken für den Bereich des Datenschutzes nicht möglich.

## Strukturelle Gewährleistung der Betroffenenrechte (Art. 12 – 22)

Die Hochschule als Verantwortliche muss gewährleisten, dass die von einer Verarbeitung ihrer personenbezogenen Daten betroffenen Personen ihre Rechte aus Art. 12 – 22 DS-GVO wahrnehmen können:

### Rechtliche Grundlage

Die Betroffenenrechte sind zentral für die Verwirklichung des Schutzes der Grundrechte für die von einer Verarbeitung ihrer personenbezogenen Daten betroffenen Personen. Die DS-GVO schafft mit den Artikeln 12 bis 22 umfangreiche Rechte für die von der Verarbeitung ihrer Daten betroffenen Personen und setzt dem Verantwortlichen für die Beantwortung oder Reaktion in Art. 12 Abs. 3 DS-GVO eine Frist von einem Monat, die aber unter gewissen Umständen (Aufgrund der Komplexität oder durch die Anzahl der Anfragen) um zwei weitere Monate verlängert werden kann. Innerhalb dieser Fristen müssen die folgenden Betroffenenrechte für die Hochschule umsetzbar sein:

#### Information bei der Erhebung direkt bei der betroffenen Person (Art. 13)

Jede natürliche Person ist zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten umfassend über die beabsichtigte Verarbeitung zu informieren. Neben der Erhebung gilt dies auch für eine Weiterverarbeitung für andere Zwecke, die nicht zum Zeitpunkt der Erhebung festgelegt waren. Eine Information kann gemäß Abs. 4 unterbleiben, wenn die betroffene Person bereits über die Information verfügt, was insbesondere der Fall ist, wenn die Erhebung aufgrund Art. 6 Abs. 1 Buchstaben c, e DS-GVO erfolgt, was bei der Hochschule in Ausübung ihrer gesetzlich gegebenen Aufgaben regelmäßig der Fall ist. Auch ohne eine Pflicht zur Angabe der Information ist es ratsam, bei der Erhebung auf die der Erhebung und Verarbeitung zugrundeliegende Rechtsnorm hinzuweisen, um dem Grundsatz einer fairen und transparenten Datenverarbeitung gemäß Art. 5 Abs. 1 lit. a DS-GVO nachzukommen. Zudem ist die Informationspflicht für alle freiwillig anzugebenden Daten umzusetzen, wodurch eine Information nur dann unterbleiben darf, wenn ausschließlich von der Rechtsnorm abgedeckte Daten erhoben werden und keine freiwilligen Angaben mit Bezug zu natürlichen Personen gemacht werden können. Regelmäßig begründen Rechtsnormen den anzugebenen Datensatz mit der Erforderlichkeit für die jeweilige Zweckerreichung.

Die Inhalte der bereitzustellenden Informationen werden durch Abs. 1, 2 vorgegeben. Vor einer Weiterverarbeitung zu anderen Zwecken sind gemäß Abs. 3 die Angaben nach Abs. 2 sowie Informationen zu den anderen Zwecken zur Verfügung zu stellen.

#### Abs. 1: Grundangaben

1. Name und Kontaktdaten des Verantwortlichen: Quelle der Information ist Punkt a) im Verzeichnis der Verarbeitungstätigkeiten (VVT).
2. Kontaktdaten des oder der Datenschutzbeauftragten: Quelle der Information ist Punkt a) im VVT.
3. Die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlagen für die Verarbeitung: Die Zwecke können Punkt b) im VVT entnommen werden. Für die Rechtsgrundlage ist ein Erlaubnistatbestand aus Art. 6 Abs. 1 DS-GVO zu erwähnen sowie ggf. die verpflichtende Rechtsnorm.
4. Sofern die Erhebung auf Grundlage von Art. 6 Abs. 1 Buchstabe f DS-GVO erfolgt, die berechtigten Interessen die von einem Verantwortlichen oder einem Dritten verfolgt werden: Für die Einhaltung des Grundsatzes einer fairen und transparenten Verarbeitung unter dem Aspekt von Treu und Glauben ist eine Interessenabwägung erforderlich. Damit kann die betroffene Person sich eine Einschätzung bzgl. der Durchsetzbarkeit ihres Rechts auf Widerspruch gemäß Artikel 21 DS-GVO bilden.
5. Die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten: Quelle der Information ist Punkt d) im VVT.
6. Die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln: Quelle der Information ist Punkt e) im VVT.

#### Abs. 2: Weitere Informationen, die eine faire und transparente Verarbeitung gewährleisten

1. Die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die die Kriterien für die Festlegung dieser Dauer: Quelle der Information ist Punkt f) im VVT.
2. Das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit.
3. Wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird: Durch diese Angabe werden die Bedingungen aus Art. 7 Abs. 3 Satz 3 DS-GVO erfüllt. Neben den rechtlichen Randbedingungen, wie den Folgen des Widerrufs, muss auch darauf hingewiesen werden, auf welchem Weg die betroffene Person ihr Widerrufsrecht unter Berücksichtigung von Art. 7 Abs. 3 Satz 4 DS-GVO ausüben kann. Die Umsetzung erfolgt im Rahmen der Informationen im Zusammenhang mit der Einwilligung (Einwilligungserklärung).
4. Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde: Betroffene Personen haben gemäß Art. 77 DS-GVO das Recht, jederzeit eine Datenschutz-Aufsichtsbehörde anzurufen, wenn sie der Ansicht sind, eine Verarbeitung verstößt gegen die gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten. Daher ist es sinnvoll, direkt die zuständige Datenschutz-Aufsichtsbehörde anzugeben.
5. Ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte: Diese Angaben erläutern die Angabe der Rechtsgrundlage aus Absatz 1 Punkt c). Bei gesetzlich vorgeschriebenen Daten sollte die genaue Fundstelle im Gesetz angegeben werden, damit sich die betroffene Person umfassend informieren kann.
6. Das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person: Damit die betroffenen Personen ihr Recht auf Eingreifen einer Person seitens des Verantwortlichen in die automatisierte Entscheidungsfindung, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gemäß Art. 22 Abs. 3 DS-GVO ausüben können, müssen sie darüber informiert sein, und in die Lage versetzt werden, die automatisierte Entscheidungsfindung nachvollziehen zu können, um eventuelle Fehlberechnungen oder die Verarbeitung unrichtiger Daten anzumerken.

**Dokumente:**

* Ankreuzbare Checkliste zur Erleichterung der Zusammenstellung der Informationen für die jeweilige Verarbeitung.

### Umsetzung der Informationspflicht bei der Erhebung

#### Datenschutzerklärung Internetseite

Bei der Bereitstellung einer Internetseite[[1]](#footnote-1) werden mindestens bei der technischen Bereitstellung IP-Adressen und ggf. weitere personenbeziehbare Angaben aus dem http-Request verarbeitet. Daher ist eine Zurverfügungstellung der oben aufgeführten Informationen erforderlich. Die Datenschutz-Aufsichtsbehörden haben dazu angemerkt, dass es genügt, die Angaben auf eine Seite zum Thema „Verarbeitung personenbezogener Daten“ zu stellen, die von jeder Seite der Internetseite mit einem Klick erreichbar ist, wobei der Link eindeutig mit „Datenschutz“ oder „Verarbeitung personenbezogener Daten“ beschriftet sein muss. In der Regel werden bei Internetseiten Angaben zu den folgenden Zwecken gemacht werden müssen:

* **Protokollierung**: In der Regel werden Zugriffe auf den Webserver protokolliert, wobei eine Anonymisierung der IP-Adresse denkbar ist. Für Fehlerlogs ist dagegen die Angabe der vollständigen IP-Adresse erlaubt, sofern durch kurze Aufbewahrungsfristen, eng begrenzte Zugriffsberechtigungen und strikte Zweckbindung eine rechtskonforme Datenverarbeitung erfolgt.
* **Webanalytik**: Sofern ein Tool wie Matomo (vormals Piwik) zur Analyse des Besucherverhaltens auf der Internetseite eingesetzt wird, müssen entsprechende Informationen zur Software bereitgestellt werden. An dieser Stelle muss explizit eine ausführliche Anleitung zum Opt-out sowie ggf. zur Anonymisierung der Daten angegeben werden. Außerdem muss darauf hingewiesen werden, was eine Löschung des Opt-out-Cookies bewirkt. Eine Nutzung von Drittanbietern (insbesondere Google Analytics) kann nur erfolgen, wenn der Besucher der Übermittlung aktiv zugestimmt hat (Opt-in).
* **Social Media**: Bei der Einbindung von Social Media Accounts ist auf eine datenschutzfreundliche Ausgestaltung zu achten. Insbesondere dürfen keine Dateien (weder Skripte noch Bilddateien) direkt von den Anbietern eingebunden werden. Die Besucher müssen vor einem Klick auf die Links darauf hingewiesen werden, dass sie die Internetseite der Hochschule verlassen.
* **Drittanbieter**: Es können auch Daten von Drittanbietern direkt in die Internetseite eingebaut werden. Über diese Verwendung und dabei mögliche Verarbeitungen personenbezogener Daten (insbesondere Protokollierung, Tracking und Cookies) muss umfangreich aufgeklärt werden. Wo immer möglich sollten die Daten direkt auf einem Webserver der Hochschule abgelegt werden, damit keine Datenübertragung an Dritte erfolgt.
* **Kontaktformulare**: Es werden die obigen Angaben zur Information direkt neben dem Kontaktformular erwartet. Wichtige Angaben sind zudem die Verwendung von Transportverschlüsselung sowie die Aufbewahrungsfristen und die Empfänger der Nachricht.
* **Cookies**: Sofern die Internetseite Cookies verwendet, muss über jedes einzelne eingesetzte Cookie eine Information erfolgen. Dabei sind neben der Funktion und dem Zweck die verarbeiteten personenbezogenen Daten auch für technische Laien verständlich zu erklären. Dazu sind insbesondere Angaben zur Speicherdauer wichtig. Für ausgewählte Fälle (z. B. Schriftgröße, gewählte Sprache, Opt-out zur Webanalyse, Opt-in zur Webanalyse) ist die Speicherung mittels Cookie denkbar, ein generelles Tracking über Besuche hinweg mittels Benutzernummer aber nicht.
* **Dynamische Inhalte**: Sofern die Webseite dynamisch generiert wird und dabei eine Verarbeitung von Daten aus dem http-Header erfolgt, sind diese Angaben zu den Verarbeitungen zu ergänzen. Beispiele hierfür sind: Berücksichtigung der favorisierten Spracheinstellung, der Fenstergröße, des Namens des Webbrowsers mit der genauen Versionsnummer und installierter Add-ons bzw. Plug-ins. In der Regel erfolgt die Anpassung für ein gleiches Verhalten der Webseite für alle Besucher. Die Übermittlung dieser Daten ist nicht erforderlich für die Funktionalität der Internetseite. Ein Hinweis auf Abschaltung enthält die Anpassung der http-Header-Inhalte durch den Anwender in den Webbrowser-Einstellungen.

#### Datenschutzerklärung Campusmanagementsystem (CMS)

Im öffentlich einsehbaren Teil des CMS muss nur über die Verarbeitung personenbezogener Daten im öffentlich einsehbaren Bereich informiert werden. Die Angaben decken sich meist mit den vorstehenden Angaben bei einer Internetseite.

Für die im Rahmen der Benutzerregistrierung zu machenden Angaben wird auf den nachfolgenden Abschnitt verwiesen. Dies betrifft insbesondere Angaben bei der Bewerberregistrierung für Studierende und Mitarbeiter sowie bei der Verwaltung Ehemaliger und bei einem möglichen Weiterbildungsangebot für Berufstätige.

Für die zugriffsgeschützten Bereiche sollten die Angaben wie für eine Internetseite bereitgestellt werden, sowohl vom Inhalt als auch von der Erreichbarkeit. Es muss zudem darauf eingegangen werden, wie die Daten anonymisiert werden, weil durch den erfolgten Log-in ein direkter Personenbezug möglich ist. Da die Verarbeitung auf gesetzlichen Grundlagen erfolgt, ist eine Information der betroffenen Personen für die nachfolgenden Verarbeitungszwecke nicht erforderlich. Ein Hinweis auf die gesetzlichen Erlaubnisnormen ist allerdings sinnvoll, um eine transparente und faire Verarbeitung personenbezogener Daten zu gewährleisten: Bewerbung auf Studienplätze, Studierendenverwaltung, Lehrveranstaltungsverwaltung, Prüfungsverwaltung.

#### Automatischer Log-in

Sofern eine Funktion zum automatischen Log-in auf (mobilen) Geräten verwendet wird, muss vor der Datenerhebung im Log-in-Formular auf die Funktionsweise der Verarbeitung, Speicherung von Daten auf dem Endgerät des Benutzers (Cookie), Speicherung von gerätebezogenen Daten in dem CMS sowie möglicher Gefahren hingewiesen werden und eine aktive Bestätigung (z. B. Markieren einer Checkbox oder Klicken auf speziellen Button) der betroffenen Person eingeholt werden.

Als Rechtsgrundlage wird Art. 6 Abs. 1 Buchstabe a) DS-GVO zur Anwendung kommen. Damit ist die betroffene Person explizit auf ihr Widerrufsrecht hinzuweisen.

#### Erhebung bei der Benutzerregistrierung

Sofern die Erhebung digital durchgeführt wird, werden die oben aufgeführten Informationen vollumfänglich und unübersehbar vor Beginn der Registrierung eingeblendet.

#### Datenschutzerklärung E-Learning-Software (ELS)

Die Anforderungen an eine E-Learning-Software basieren auf den Angaben für eine Internetseite. Jedoch müssen die Verarbeitungen personenbezogener Daten um Funktionalitäten der ELS ergänzt werden.

#### Erhebung im Rahmen von Tel*e*fona*n*rufen

Sofern im Rahmen von Telefonanrufen (z. B. Hotline, Studierendensekretariat, Prüfungsamt) eine Erhebung oder Verarbeitung personenbezogener Daten erfolgen kann, wird die betroffene Person im Rahmen des Telefonats aufgeklärt. Dies erfolgt durch einen deutlichen und expliziten Hinweis (z. B. auch durch eine Bandansage), wo die Informationen aufzufinden sind (in der Regel im CMS) und durch eine verkürzte Darstellung in mündlicher Form.

#### Erhebung in Papierform

Die Anforderungen aus der DS-GVO erstrecken sich nur dann auf die papiergebundene Erhebungen personenbezogener Daten, wenn diese Daten später in eine automatisierte Verarbeitung übertragen werden. Dies ist z. B. dann der Fall, wenn Daten mit einem Papierformular erhoben werden, diese aber durch die Sachbearbeiter anschließend elektronisch erfasst und weiterverarbeitet werden.

#### Erhebung und Verarbeitung in Forschungsprojekten

Bei der Erhebung für Forschungsprojekte gelten im Prinzip die gleichen Anforderungen, wobei es davon abhängt, welche Daten bei wem erhoben werden. Für eine Umfrage werden der Person vor Beginn der Umfrage die erforderlichen Informationen bereitgestellt.

#### Datenschutzerklärung bei der Verwaltung Ehemaliger

Sofern die Verwaltung ehemaliger Studierender und Mitarbeiter eine gesetzliche Aufgabe der Hochschule ist, gelten die Anforderungen wie bei einem Campusmanagementsystem.

Sollte es sich um eine auf Einwilligung basierende Verarbeitung handeln, werden die Informationen im Rahmen des Einwilligungstextes zur Verfügung gestellt.

### Information bei der Erhebung bei Dritten (Art. 14)

Dieser Fall sollte an der Hochschule eher selten vorkommen. Sofern personenbezogene Daten nicht direkt bei der betroffenen Person erhoben wurden, ist die betroffene Person nach Maßgabe von Art. 14 umfassend über die Daten und die Datenverarbeitung zu informieren. Eine Information der betroffenen Person kann gemäß Abs. 5 unterbleiben, wenn die betroffene Person bereits über die Information verfügt, was insbesondere der Fall ist, wenn die Verarbeitung der personenbezogenen Daten aufgrund Art. 6 Abs. 1 Buchstaben c, e DS-GVO erfolgt, was bei Behörden in Ausübung ihrer gesetzlich gegebenen Aufgaben regelmäßig der Fall ist.

Die Inhalte der der betroffenen Person bereitzustellenden Informationen werden durch Art. 14 Abs. 1, 2 DS-GVO konkretisiert. Vor einer Weiterverarbeitung zu anderen Zwecken sind den betroffenen Personen gemäß Abs. 4 die Angaben nach dem zweiten Absatz sowie Informationen zu den anderen Zwecken zur Verfügung zu stellen.

#### Abs. 1:

Die Angaben entsprechen denen aus Absatz 1 bei der Direkterhebung, mit folgender Ersetzung:

1. die Kategorien personenbezogener Daten, die verarbeitet werden: Quelle der Information ist Punkt c) im VVT.

#### Abs. 2:

Die Angaben entsprechen denen aus Absatz 1 bei der Direkterhebung, mit folgender Ersetzung:

1. Aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen: Im Zuge einer fairen und transparenten Verarbeitung muss die betroffene Person wissen, woher die verarbeitende Stelle die personenbezogene Daten erhalten hat, um damit in Erfahrung bringen zu können, auf welcher Rechtsgrundlage die Offenbarung von der Quelle zum Empfänger stattgefunden hat und ob die Quelle sich bei der Erhebung und Verarbeitung datenschutzrechtskonform verhalten hat. Sollte es sich um eine öffentlich zugängliche Quelle handeln, so wird die betroffene Person in die Lage versetzt, ihr Recht auf Vergessenwerden gegenüber der Quelle durchzusetzen.

Außerdem wird hinter Buchstabe a) folgende zusätzliche Information gefordert:

1. Die Angaben gemäß Absatz 1 Punkt d) bei der Direkterhebung.

### Umsetzung der Informationspflicht

#### Empfangen der Bewerbungsinformationen von Personaldienstleistern

Es ist davon auszugehen, dass Personaldienstleister bereits ihre Kunden über die Übermittlung informiert haben. Daher ist keine Information erforderlich.

#### Empfangen der Bewerbungsinformationen ausländischer Studierender über Dienstleister

Auch in diesem Fall ist keine Information erforderlich, da die Dienstleister in der Pflicht sind, die Kunden über die Datenübermittlung zu informieren. Die Hochschule kann somit davon ausgehen, dass die betroffenen Personen bereits über die Information verfügen.

#### Empfangen der Daten für Zwecke der wissenschaftlichen oder historischen Forschung

Gemäß Art. 89 Abs. 1 DS-GVO gilt eine Weiterverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken nicht als Zweckänderung, sofern geeignete Garantien zum Einsatz kommen, um die Rechte und Freiheiten der betroffenen Personen zu schützen.

### Auskunft (Art. 15)

Das Recht auf Auskunft ist die Grundlage für die Ausübung aller intervenierenden Betroffenenrechte, da eine natürliche Person nur dann ihre Rechte als von der Verarbeitung ihrer personenbezogenen Daten betroffene Person ausüben kann, wenn sie als Person in der Lage ist, zu erfahren, wer was über sie weiß. Nur wenn die Person erfahren kann, wer welche Daten über sie verarbeitet und zu welchen Zwecken dies erfolgt, ist sie in der Lage zu beurteilen, ob die Verarbeitung rechtmäßig ist. Zentral ist daher zunächst die Aussage durch den Verantwortlichen, ob überhaupt Daten mit Bezug zu der Person verarbeitet werden. An dieser Stelle ist entscheidend, den Bezug zwischen realer Person und den in der automatisierten Verarbeitung verwendeten Personenidentitäten herstellen zu können. Auf die damit zusammenhängende Problematik wird im Abschnitt Identität des Betroffenen eingegangen.

Neben dem Recht auf Auskunft, ob Daten mit Bezug zu ihrer Person verarbeitet werden, hat jede Person durch Abs. 3 das Recht, eine Kopie der zu ihrer Person gespeicherten Daten zu erhalten. Diese Datenmenge wird dahingehend eingeschränkt, dass

1. die Auskunft nur für erhobene Daten angewendet werden muss und daher nicht für Ergebnisse der Verarbeitung dieser Daten, und
2. gemäß Abs. 4 keine Daten mit Bezug zu anderen Personen herausgegeben werden dürfen, da andernfalls deren Rechte und Freiheiten beeinträchtigt wären, und
3. gemäß § 12 Abs. 2 S. 2 DSG NRW die betroffene Person keine Auskunft über die Verarbeitung sie betreffender personenbezogener Daten verlangen kann, soweit die Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und die Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

Sofern es für Verfahren die Möglichkeit einer Selbstauskunft gibt, wird die anfragende Person hierüber informiert. Bei künftigen Ausschreibungen oder Neuanschaffungen von Softwarelösungen muss darauf geachtet werden, entsprechende Selbstauskunftsfunktionen den betroffenen Personen zur Verfügung zu stellen (Datenschutz durch Technikgestaltung).

Durch Bereitstellung einer Kopie ihrer verarbeiteten, personenbezogenen Daten sowie der Angaben gemäß Abs. 1 Halbsatz 2 wird die betroffene Person in die Lage versetzt, den Eingriff in das Grundrecht nach Erwägungsgrund 1 zu verstehen und unrechtmäßige Datensätze und nicht rechtskonforme Verarbeitungen zu beanstanden und durch den Verantwortlichen korrigieren zu lassen.

Neben dem Problem des Identitätsnachweises (siehe auch Seite 30 Identität des Betroffenen und Authentizität der Anfrage) sind drei sich gegenseitig beeinflussende Faktoren Herausforderungen bei der Bereitstellung einer Kopie aller mit Bezug zu einer natürlichen Person verarbeiteten Daten:

1. die Heterogenität der Systemlandschaft an der Hochschule,
2. die Vielzahl zu einer Person in unterschiedlichen Systemen verarbeiteten Daten und
3. das datenschutzrechtliche Gewährleistungsziel der Nichtverkettbarkeit personenbezogener Daten, das die systemische Trennung von personenbezogenen Daten fordert, die zu unterschiedlichen Zwecken verarbeitet werden.

Die Hochschule ist somit, um die fristgerechte Beantwortung der Anfrage aus Ausübung ihrer Betroffenenrechte zu ermöglichen, auf die Unterstützung der anfragenden Person angewiesen, die zu beauskunftenden Verarbeitungen zu präzisieren. Dementsprechend bezieht sich die Hochschule regelmäßig auf Erwägungsgrund 63 Satz 7, sofern sich die Verarbeitungsvorgänge nicht einschränken lassen. Diese Mitwirkungspflicht bei der Verarbeitung einer großen Menge von Informationen über die betreffende Person spiegelt sich in der Regelung des § 12 Abs. 1 DSG NRW wieder. In Abs. 1 Satz 2 wird zudem klargestellt, dass das Auskunftsrecht voraussetzt, dass die Person Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglicht.

### Berichtigung (Art. 16)

Jede natürliche Person hat das Recht, unrichtige personenbezogene Daten mit Bezug zu ihrer Person vom Verantwortlichen korrigieren und unvollständige Datensätze vervollständigen zu lassen. Dies setzt voraus, dass die Person ihr Recht auf Auskunft ausüben kann, denn nur dann ist sie in der Lage, unrichtige oder unvollständige Daten mit Bezug zu ihrer Person zu erkennen.

Die Berichtigung oder Vervollständigung beziehen sich ausschließlich auf personenbezogene Fakten. Für Wertungen oder Bewertungen gilt das Recht auf Berichtigung nur für die Eingabe in die automatisierte Datenverarbeitung. Das Recht ermöglicht keine Anfechtungen von Prüfungsergebnissen, im Rahmen der Vergabe von Studienplätzen oder Belegung von Lehrveranstaltungen. Einzig bei der Ablehnung aufgrund nicht erfüllter Voraussetzungen kann mithilfe des Rechts auf Berichtigung nach erfolgter Korrektur unrichtiger oder durch Ergänzung unvollständiger Daten eine Neubewertung angestrebt werden.

Das Recht auf Berichtigung ist – ebenso wie das Recht auf Löschung – kein rein reaktives, durch die betroffene Person zu reklamierendes Recht. Vielmehr liegt es auch im Interesse der Hochschule, unrichtige und wissentlich unvollständige Daten durch Erhebungen zu korrigieren. Dies wird durch den Grundsatz Richtigkeit nach Art. 5 Abs. 1 Buchstabe d DS-GVO bekräftigt.

### Löschung und Recht auf Vergessenwerden (Art. 17)

Das Recht auf Löschung personenbezogener Daten wird zum einen durch das explizite Betroffenenrecht zum anderen durch die Grundsätze *Datenminimierung* und *Speicherbegrenzung* aus Art. 5 Abs. 1 Buchstaben c bzw. e DS-GVO gesetzlich verankert. Demnach sind personenbezogene Daten zu löschen bzw. die eine Identifizierung der betroffenen Person ermöglichenden Datensätze dauerhaft zu entfernen, sobald der Verarbeitungszweck erloschen ist oder die Daten für die Erreichung des Verarbeitungszwecks nicht mehr erforderlich sind. Die Löschpflicht gilt demnach auch für Teildatensätze, mit der Folge, dass für jedes einzelne Datum eine Löschfrist bestimmt werden muss. Es ist demnach nicht legitim, alle personenbezogenen Daten weiter zu speichern, bis die Abbildung der Personenidentität im Verarbeitungssystem der betroffenen Person an sich gelöscht werden muss.

**Die Hochschule wird ein Löschkonzept erarbeiten, aus dem hervorgeht, welche Datensätze welchen Aufbewahrungsfristen mit welchem Stichtag unterliegen, um daraus Löschroutinen zu entwickeln.**

Das Recht auf Löschung personenbezogener Daten bezieht sich auf die unrechtmäßig – insbesondere auf Grund einer (inzwischen) fehlenden Rechtsgrundlage – verarbeiteten Daten sowie auf diejenigen Daten, die die Hochschule – als Ausnahmefall − mittels einer Einwilligung verarbeitet werden. Auf letztere wirkt sich das Recht auf Löschung gemeinsam mit dem Recht auf Widerruf der Einwilligung aus. Durch den Widerruf entfällt die Einwilligung als Rechtsgrundlage.

Sofern die Hochschule personenbezogene Daten, die einem Löschanspruch unterliegen, veröffentlicht oder anderen Verantwortlichen offenbart hat, so ist sie (i. e. die/der Verfahrensverantwortliche) verpflichtet, alle Empfänger und diejenigen, die im Internet Hyperlinks auf die veröffentlichten Daten gesetzt haben, über den Löschverpflichtung zu informieren (Recht auf „Vergessenwerden“).

**Erforderliche Dokumente:**

* Löschkonzept mit der Festlegung von Löschfristen und einer möglichst automatisierten technischen Umsetzung (Vorrang der technischen Lösung vor einer organisatorischen mit manuellen Löschvorgängen).

### Einschränkung der Verarbeitung (Art. 18)

Das Recht auf Einschränkung der Verarbeitung ist dann anzuwenden, wenn

1. die Daten eigentlich gelöscht werden müssten, die betroffene Person die Daten für die Durchsetzung von Rechtsansprüchen benötigt oder die Löschung durch die betroffene Person abgelehnt wird. Das auslösende Ereignis kann ein Wegfall der Erforderlichkeit für die Erreichung des Verarbeitungszwecks oder die Erkenntnis einer unrechtmäßigen Verarbeitung sein.
2. Die Richtigkeit der Daten von der betroffenen Person bestritten wird oder die betroffene Person Widerspruch gemäß Art. 21 Abs. 1 DS-GVO eingelegt hat. In diesen Fällen werden die Daten vorübergehend gesperrt, bis der Verantwortliche die Richtigkeit der Daten überprüft bzw. die berechtigten Gründe des Verantwortlichen für die Verarbeitung gegenüber denen der betroffenen Person abgewogen hat.

Die Einschränkung der Verarbeitung muss unverzüglich umgesetzt werden, wobei eine Verarbeitung der gesperrten Daten nicht mehr durchgeführt werden darf. Die Einschränkung der Verarbeitung betrifft ausschließlich die ausgewählten personenbezogenen Daten. Alle Daten, die nicht der Einschränkung der Verarbeitung unterliegen, dürfen weiterhin für die jeweiligen Verarbeitungszwecke verwendet werden.

### Datenübertragbarkeit (Art. 20)

Mit dem Recht auf Datenübertragbarkeit soll es betroffenen Personen ermöglicht werden, den Anbieter oder Dienstleister vereinfacht zu wechseln, indem ein Anspruch gegenüber dem bisherigen Anbieter besteht, die dortigen Kundendaten in einem portablen Format zu einem neuen Anbieter oder Dienstleister mitzunehmen. Das Recht beschränkt sich dabei auf diejenigen Daten, die von der betroffenen Person bereitgestellt wurden, und schließt Erhebungen bei Dritten, Bewertungen und Ergebnisse von (automatisierten) Verarbeitungen aus. Ebenfalls dürfen gemäß Abs. 4 durch die direkte Übertragung von einem Anbieter zu einem anderen Anbieter die Rechte und Freiheiten anderer natürlicher Personen nicht beschränkt werden.

Das Recht auf Datenübertragbarkeit ist nur für diejenigen Daten anzuwenden, die aufgrund einer Einwilligung oder eines Vertrags zwischen Verantwortlichem und der betroffenen Person verarbeitet wurden. Im Bereich ihrer Aufgabenerfüllung wird die Hochschule üblicherweise auf Grundlage einer gesetzlichen Aufgabenbeschreibung und Pflicht zur Datenverarbeitung agieren, weswegen das Recht auf Datenübertragbarkeit keine Anwendung auf diese Bereiche findet. **Somit ist das Recht auf Datenübertragbarkeit auf den gesamten Student-Life-Cycle nicht anwendbar.**

Die Datenverarbeitung auf Rechtsgrundlage nach Art. 6 Abs. 1 Buchstaben a) (Einwilligung) und b) (Vertrag) DS-GVO trifft im Bereich der Hochschule nur zu

1. auf freiwillig angegebene Daten oder zusätzlich in Anspruch genommene Dienstleistungen wie Ehemaligenverwaltung zu, da die Hochschule als öffentliche Stelle auf gesetzlichen Rechtsgrundlagen personenbezogene Daten verarbeitet, sowie
2. auf personenbezogene Daten zu, die im Rahmen eines Weiterbildungsstudiums für Externe/Berufstätige oder bei Angeboten des Hochschulsports auf Grundlage eines Vertrags verarbeitet werden.
3. auf Fitnessangebote des Hochschulsports an die Allgemeinheit, die dann ebenfalls auf einer vertraglichen Grundlage erfolgen.

Prinzipiell könnte auch eine Relevanz im Bereich von Forschungsprojekten bestehen, wenn die Daten des Betroffenen aufgrund einer Einwilligung verarbeitet werden. Allerdings ist dort in der Regel nicht die Interessenlage aus Art. 20 DS-GVO bei der betroffenen Person gegeben

**Erforderliche Dokumente:**

* Konzept für die Umsetzung des Rechts auf Datenübertragbarkeit für die genannten relevanten Fälle.

### Widerspruch (Art. 21)

Bei Verarbeitungen personenbezogener Daten, die aufgrund Art. 6 Abs. 1 Buchstaben e oder f DS-GVO erfolgen, haben davon betroffene Personen ein durch Art. 21 verwirklichtes Widerspruchsrecht, wobei sich die Gründe aus der besonderen Situation der jeweiligen Person ergeben. Bei eingelegtem Widerspruch ist es Aufgabe des Verantwortlichen, durch eine Interessensabwägung zwischen der besonderen Situation der betroffenen Person sowie den zwingenden schutzwürdigen Gründen des Verantwortlichen durchzuführen. Dabei müssen die Gründe des Verantwortlichen die Interessen, Rechte und Freiheiten der betroffenen Personen überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Gemäß Abs. 6 kann ein Widerspruch auch gegen die Verarbeitung für wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke nach Art. 89 Abs. 1 eingelegt werden, sofern die Verarbeitung nicht zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

### Automatisierte Entscheidung im Einzelfall (Art. 22)

Entscheidungen mit rechtlichen Wirkungen oder Beeinträchtigungen für die betroffenen Personen dürfen nicht auf einer ausschließlich automatisierten Verarbeitung beruhen. Daher ist es unabdingbar, dass die Veröffentlichung von Ergebnissen automatisierter Verfahren wie Vergabe von Studienplätzen, Belegung von Veranstaltungen und Exmatrikulation aufgrund Verstoßes gegen die Prüfungsordnung einer manuellen Kontrolle durch Sachbearbeiter unterliegen. Der manuelle Eingriff (die Kontrolle der Entscheidung) ist dementsprechend zu dokumentieren und der oder dem Datenschutzbeauftragten auf Anforderung zur Verfügung zu stellen.

### Verantwortlichkeit / Zuständigkeit

|  |  |  |
| --- | --- | --- |
|  | Verantwortlich | Zuständig für die Umsetzung |
| Gesamtverantwortung | Hochschulleitung | |
| Auskunft, Berichtigung, Durchführung der Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit | Fachabteilung oder fachlich verantwortliche Person für die Verarbeitung (fvP) | |
| Weiterleitung der Anfrage an zuständige Fachabteilung bzw. an verantwortliche Person | bDSB (wenn der Betroffene die Anfrage an diesen gerichtet hat) | |
| Erarbeitung und Umsetzung Löschkonzept | Hochschulleitung | Fachabteilung unter Einbeziehung des Personalrats und des bDSB |
| Widerspruch | Fachabteilung, fvP | Fachabteilung, fvP  Ablehnende Entscheidung muss mit der Stabsstelle oder der internen Kompetenzstelle Recht getroffen und begründet werden |
| Automatisierte Entscheidung im Einzelfall | Fachabteilung, fvP | Fachabteilung, fvP  gegenüber bDSB auf Anfrage berichtspflichtig |
| Überwachung der Einhaltung der gesetzlichen Anforderungen | bDSB | bDSB mit Bereitstellung der Information durch die Fachabteilungen und die Hochschulleitung |

### Identität des Betroffenen und Authentizität der Anfrage

Die Hochschule muss gemäß Art. 12 Abs. 6 DS-GVO sicherstellen, dass die anfragende Person auch die Person ist, die sie vorgibt zu sein. Dazu müssen ggf. weitere Daten von der anfragenden Person erhoben werden, die eine Identifizierung ermöglichen (bspw. amtliche Ausweisdokumente), da die üblichen Kanäle den datenschutzrechtlichen Anforderungen nicht angemessen sind. Hierbei sind grob zwei Fälle zu unterscheiden:

1. Für Anfragen, die von einer Hochschul-E-Mail-Adresse gestellt werden, wurde eine Identitätsprüfung bereits vollzogen und der Nachweis der Zuordnung von E-Mailadresse zu Person ist erbracht. (Je nach Gegebenheiten der Hochschule: Nach Möglichkeit werden Anfragen elektronisch signiert oder verschlüsselt, sodass ein höheres Niveau der Authentizität der Anfrage erreicht ist. Sofern personengebundene Zertifikate in der Hochschule ausgerollt sind, wird die Verwendung dieser für interne Anfragen vorgeschrieben.)
2. Für Anfragen, die mündlich, postalisch, per Fax oder von einer externen E-Mailadresse eintreffen, müssen Kopien von amtlichen, identifizierenden Dokumenten eingefordert werden. Die Auskunft wird dann postalisch an die aus den Dokumenten hervorgehende Meldeadresse erteilt.

Alternativ kann die betroffene Person im Rahmen der persönlichen Abholung bei der Fachabteilung oder der bzw. dem Datenschutzbeauftragten vorstellig werden und ihre amtlichen Dokumente vorlegen, sodass in der Verlaufsdokumentation nur der Vermerk der erfolgreichen Identitätsprüfung eingetragen werden muss.

### Technische Maßnahmen zur Gewährleistung der Betroffenenrechte

Ein wichtiger Punkt bei der gesetzeskonformen Etablierung eines Verfahrens zur Gewährleistung der Betroffenenrechte ist die Authentisierung von Anfragen. Dies wird in der DS-GVO auch in Erwägungsgrund 64 erläutert und in Art. 12 Abs. 6 DS-GVO gesetzlich verankert. Demnach obliegt es dem Verantwortlichen, die Identität der anfragenden Person zweifelsfrei bestimmen zu können und die Authentizität der Anfrage sicher zu stellen. Daraus ergeben sich Anforderungen an die Form der Anfrage. Art. 12 Abs. 1 Satz 2 DS-GVO ermöglicht die elektronische Kommunikation, ebenso fordert Art. 12 Abs. 3 Satz 4 DS-GVO die elektronische Beantwortung von elektronischen Anfragen. Allerdings sind E-Mails nicht geeignet für diese Kommunikation, da die Vertraulichkeit grundsätzlich nicht gewährleistet werden kann, weil E-Mails grundsätzlich im Klartext übertragen werden und daher von E-Mail­pro­vi­dern und Netzbetreibern mitgelesen werden können. Daher wird das Verfahren folgendermaßen technisch abgebildet:

1. Die E-Mailadresse <datenschutzanfragen@hochschule.X.de> ist an ein (bestehendes, z.B. Incident Handling des Hochschulrechenzentrum) Trouble-Ticket-System (TTS, z. B. OTRS) angebunden und per E-Mail einkommende Anfragen werden in eine spezielle Queue einsortiert, auf die ausschließlich Personen Zugriff haben, die in die Beantwortung von Anfragen involviert sind. Diese Personengruppe umfasst die Mitarbeiter im Datenschutzmanagement als auch die oder der Datenschutzbeauftragte und deren Stellvertreter. die / die / Der Vorteil eines TTS liegt in der Prozessunterstützung, der automatischen Erinnerung bzw. Eskalation und der Unterstützung von E-Mail-Signatur und -Verschlüsselung sowie der Revisionssicherheit. Daher können Anfragen, die digital signiert und ggf. verschlüsselt wurden, automatisch mit verschlüsselten E-Mails beantwortet werden. Gleichzeitig können hierüber automatisiert ein Aktenzeichen vergeben, der Bearbeitungszustand verwaltet und Aufgabenlisten sowie Wiedervorlagen erzeugt werden.
2. Weiterhin wird ein Kunden-Frontend benötigt, über das Anfragen gestellt und Nachweise erbracht werden können. Diese Daten werden über eine verschlüsselte Verbindung an das TTS übertragen. Hierüber können anfragende Personen (zeitlich begrenzt) Einsicht in ihre Anfragen nehmen.
3. An die zur Registrierung verwendete E-Mailadresse werden ausschließlich neutrale Hinweismails auf neu hinterlegte Informationen verschickt. Es erfolgt keine Übertragung von Inhalten oder gar Kopien personenbezogener Daten.
4. Bei ausgewählten Diensten (z. B. Bewerber-, Studierenden- und Prüfungsverwaltung) wird eine Selbstauskunft für die betroffene Person nach der Maßgabe von Art. 15 DS-GVO eingebaut. Dabei werden die dort gespeicherten Daten für die angemeldete Person aufbereitet.
5. Per Briefpost, Fax oder mündlich gestellte Anfragen werden ebenfalls im Ticketsystem erfasst, damit alle Anfragen von einem zentralen System aus verwaltet werden. In diesen Fällen sollte dann die Antwort postalisch an die Meldeadresse zugestellt werden, wenn die Identität der Person zweifelsfrei geklärt werden konnte.

### Ablehnung, Fristverlängerung und Information hierüber

Die Hochschule kann in wenigen Fällen die Ausübung der Rechte unterlassen, wobei die Gründe zu dokumentieren und ggf. nachzuweisen sind:

1. Dies kann gemäß Art. 12 Abs. 2 Satz 2 DS-GVO dann der Fall sein, wenn die Hochschule nicht in der Lage ist, die Daten mit Bezug zu der betroffenen Person aufzufinden, weil diese ohne Personenbezug gespeichert wurden oder der Personenbezug nach Zweckende gemäß Art. 5 Abs. 1 Buchstabe e) DS-GVO entfernt wurde.
2. Es gibt zu dokumentierende Anhaltspunkte, dass von einer betroffenen Person exzessiv viele gleiche oder ähnliche Anträge gestellt werden, deren Häufigkeit keine Begründung zugrunde liegt. In diesen Fällen kann die Hochschule entweder ein angemessenes Entgelt verlangen oder sich weigern, die Anfrage zu erfüllen.

Der anfragenden Person wird gemäß Art. 12 Abs. 4 DS-GVO über ihr Beschwerderecht bei einer Datenschutz-Aufsichtsbehörde informiert. Da die oder der behördliche Datenschutzbeauftragte gemäß Art. 39 Abs. 1 Buchstabe e DS-GVO als Anlaufstelle für die Aufsichtsbehörde fungiert, muss dieser über den Fall und die ablehnende Entscheidung informiert werden. Ebenso wird die oder der behördliche Datenschutzbeauftragte in Fällen der Fristverlängerung gemäß Art. 12 Abs. 3 DS-GVO informiert.

### Kontrolle und Überwachung der Gewährleistung der Betroffenenrechte

Die Kontrolle der Gewährleistung der Betroffenenrechte ist Aufgabe der oder des behördlichen Datenschutzbeauftragten gemäß Art. 39 Abs. 1 Buchstabe b DS-GVO. Diesem werden die erforderlichen Ressourcen, insbesondere in zeitlichem Budget, Unterstützung durch die Verfahrensverantwortlichen und Zugang zu Dokumentation der Anfragenbearbeitung ohne Verzögerung bereitgestellt.

Die oder der Datenschutzbeauftragte unterrichtet die Hochschulleitung regelmäßig über die Einhaltung der Vorgaben zur Gewährleistung der Betroffenenrechte und kann bei mangelhafter Umsetzung jederzeit von der Hochschulleitung Nachbesserungen und die Einhaltung der gesetzlichen Vorgaben verlangen. Die Ergebnisse der Kontrollen sowie angepasste Anforderungen aus gesetzgeberischer Sicht werden regelmäßig in den Prozess eingearbeitet und dokumentiert.

## Strukturelle und organisatorische Sicherstellung der Meldepflichten aus Art. 33 und 34 DS-GVO

### Rechtliche Grundlagen

Bei Datenpannen handelt es sich um Verletzungen des Schutzes personenbezogener Daten, aus denen Gefährdungen (Risiken) für die Rechte und Freiheiten der natürlichen Personen entstehen können. Für derartige Schutzverletzungen sieht die DS-GVO in den Artikeln 33 und 34 Melde- und Benachrichtigungspflichten gegenüber der zuständigen Datenschutz-Aufsichtsbehörde bzw. den betroffenen Personen vor:

* Die Meldung nach Artikel 33 gegenüber der Datenschutz-Aufsichtsbehörde darf nur unterbleiben, wenn die Schutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
* Die Benachrichtigung nach Artikel 34 gegenüber den von der Datenpanne betroffenen Personen muss nur erfolgen, wenn die Schutzverletzung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt oder die Aufsichtsbehörde dies gemäß Abs. 4 anordnet. Die Benachrichtigung muss nicht erfolgen, wenn gemäß Abs. 3 eine der folgenden Bedingungen erfüllt ist oder die Datenschutz-Aufsichtsbehörde mit einem Beschluss gemäß Abs. 4 feststellt, dass eine Bedingung erfüllt ist:
  1. Geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen wurden, womit die von der Schutzverletzung betroffenen personenbezogenen Daten für unbefugte Personen unzugänglich gemacht wurden.
  2. Durch Maßnahmen (z. B. Verschlüsselung) wurde sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht.
  3. Sollte die individuelle Benachrichtigung der betroffenen Personen mit einem unverhältnismäßigen Aufwand verbunden sein, so kann die Benachrichtigung auch durch öffentliche Bekanntmachung oder ähnliche Maßnahmen erfolgen, die die betroffenen Personen vergleichbar wirksam informiert.

Die Meldung nach Artikel 33 muss unverzüglich, aber innerhalb von 72 Stunden nach Bekanntwerden erfolgt sein, andernfalls ist eine Begründung für die Verzögerung beizufügen. Die Benachrichtigung nach Artikel 34 muss unverzüglich erfolgen. Der Beginn der Frist ist der Zeitpunkt, zu dem eine angestellte oder beschäftigte Person der Hochschule von der Datenpanne erfährt.

Die inhaltlichen Anforderungen an die beiden Meldungen sind ähnlich, wobei bei der Benachrichtigung die Art der Schutzverletzung in klarer und einfacher Sprache erfolgen soll, wohingegen bei der Meldung die Beschreibung der Schutzverletzung in Fachsprache erfolgen kann und weitere Details wie Kategorien und ungefähre Zahl der betroffenen Personen sowie Kategorien und ungefähren Zahl betroffener Datensätze anzugeben sind. Die weiteren Angaben innerhalb der Meldung bzw. Benachrichtigung sind gemäß Art. 33 Abs. 3 bzw. Art. 34 Abs. 2 DS-GVO:

1. Name und Kontaktdaten der oder des Datenschutzbeauftragten oder einer Anlaufstelle
2. Beschreibung der wahrscheinlichen Folgen der Schutzverletzung
3. Beschreibung der
   1. ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Schutzverletzung und
   2. gegebenenfalls Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen.

Eine Meldung durch Auftragsverarbeiter an die Verantwortlichen muss gemäß Artikel 33 Abs. 2 DS-GVO ebenfalls unverzüglich erfolgen, wobei an diese Meldung keine weiteren gesetzlichen Anforderungen oder Bedingungen geknüpft sind. Diese ergeben sich aber indirekt aus den oben erwähnten Angaben zur der Art der Schutzverletzung und den ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Schutzverletzung und Abmilderung möglicher nachteiliger Auswirkungen. Die Hochschule berücksichtigt diese Anforderungen in Verträgen zu Auftragsverarbeitungen mit den entsprechenden Auftragnehmern. Ist die Hochschule selbst Auftragsverarbeiter, wird der Fachbereich bzw. die fachlich verantwortliche Person auf diese Pflichten gegenüber den Auftragnehmern hingewiesen.

### Verantwortlichkeiten

Jede angestellte oder beschäftigte Person an der Hochschule hat die Pflicht, mögliche Schutzverletzungen personenbezogener Daten sofort auf den unten aufgeführten Wegen intern zu melden. Mit Kenntnis durch eine angestellte oder beschäftigte Person der Hochschule beginnt die Meldefrist.

Die Hochschulleitung übernimmt die Gesamtverantwortung für die Einhaltung der Melde- und Benachrichtigungspflicht und stellt die benötigten Ressourcen für die Erfüllung der Meldepflichten und die Beseitigung der Schutzverletzung durch technische und organisatorische Maßnahmen bereit.

Die oder der behördliche Datenschutzbeauftragte überwacht gemäß Art. 39 Abs. 1 Buchstabe b DS-GVO die Einhaltung der Melde- und Benachrichtigungspflicht. Dementsprechend stellt die Hochschule die erforderliche Dokumentation oder Zugang zu dieser unverzüglich bereit. Außerdem wird die bzw. der Datenschutzbeauftragte aufgrund seiner Expertise und Fachkenntnis für die Bewertung des Risikos konsultiert.

Der oder die Verfahrensverantwortliche ist zusammen mit dem oder der Informationssicherheitsbeauftragten für die Planung und Umsetzung von Maßnahmen zur Beseitigung der Schutzverletzung verantwortlich.

Die Bearbeitung interner und externer Meldungen von möglichen Schutzverletzungen wird durch die Stabsstelle Datenschutz durchgeführt unter Hinzunahme der jeweiligen Verfahrensverantwortlichen. Die oder der behördliche Datenschutzbeauftragte wird zur Einschätzung des Risikos zu Rate gezogen. Die Entscheidung, ob eine Meldung gegenüber der Aufsichtsbehörde und den betroffenen Personen erfolgt, wird ebenfalls durch die Stabsstelle Datenschutz getroffen und von deren Leitung bzw. der stellvertretenden Leitung durchgeführt.

Sofern es sich um eine Auftragsverarbeitung für eine andere Stelle handelt, werden die Verantwortlichen der anderen Stelle unverzüglich informiert.

### Technische und organisatorische Maßnahmen

Der Art und Schwere der Schutzverletzung wird Rechnung getragen. Die Schutzverletzungen mit höherem Risiko oder Risiko für einen größeren Personenkreis werden priorisiert gegenüber Schutzverletzungen mit voraussichtlich geringeren Ausmaßen oder Auswirkungen bearbeitet.

In Bezug auf Datenpannen, Meldepflichten und -wege muss eine möglichst weitgehende Sensibilisierung und Schulung erfolgen. In diesem Zuge wird den Teilnehmern das Wissen vermittelt, wie sie mögliche Schutzverletzungen personenbezogener Daten erkennen können und wie diese innerhalb der Hochschule zu melden sind. Es bestehen hinsichtlich des Personenkreises die folgenden Prioritäten:

* Beschäftigte im IT-Support und solche die mit sensiblen Daten oder Daten in großem Umfang umgehen (Personal-, Bewerber-, Studierenden- und Prüfungsverwaltung, Forschungsprojekte mit solchen Daten): Höchste Priorität
* Alle weiteren Angehörigen und Mitglieder der Hochschule

**Erforderliche Dokumente:**

* Sensibilisierungs- und Schulungskonzept zu den Meldepflichten

Die Meldung einer möglichen Schutzverletzung erfolgt an die Stabsstelle Datenschutz, die per E-Mail, Fax und Telefon (Sprachbox) erreichbar ist. Eine postalische Übermittlung ist auch möglich, aufgrund der zeitlichen Vorgaben an die Bearbeitung wird die elektronische Zustellung bevorzugt. Die Bearbeitung erfolgt in einem Ticketsystem, in dem auch Datenpannen erfasst werden, die nicht elektronisch gemeldet werden. Das Ticketsystem verschickt automatisiert und wiederholt Benachrichtigungen und Erinnerungen, sofern Datenpannen noch nicht gemeldet wurden, um den Prozess und die Einhaltung der Meldefrist zu unterstützen.

### Information und Schulung der Mitarbeiter (Art. 29)

Die Information, Sensibilisierung und Schulung der angestellten und beschäftigten Personen, die personenbezogene Daten verarbeiten, ist ein zentraler Baustein bei der Einhaltung der Anforderungen der DS-GVO. Nur auf diese Weise kann die Hochschule sicherstellen, dass die Grundsätze der Datenverarbeitung eingehalten werden können, denn nur wenn der Datenschutz fest in der täglichen Arbeit und im Bewusstsein aller verankert ist, wird es gelingen, das Datenschutzniveau kontinuierlich zu steigern.

Zur Sensibilisierung und Schulung werden die folgenden Maßnahmen implementiert:

* Erstinformation und Verpflichtung jeder mit der Verarbeitung personenbezogener Daten zu beschäftigende Person bei der Einstellung auf Einhaltung der gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten durch die Personalabteilung. Dies entspricht der Verarbeitung ausschließlich auf Weisung des Verantwortlichen bzw. gesetzlicher Verpflichtungen und Befugnisse zur Verarbeitung gemäß Art. 29 und Art. 32 Abs. 4 DS-GVO.
* Regelmäßige, verpflichtende Schulungen für alle angestellten und beschäftigten Personen
* Aufbau und Bewerbung eines Abschnitts im Intranet, der sich mit Informationen zu Datenschutzfragen befasst, bspw.
  + Informationsmaterial zu Grundsätzen der Verarbeitung personenbezogener Daten
  + Merkblätter für (spezielle) Verarbeitungskontexte inkl. Rechtsgrundlagen und Zweckbindung
  + Checklisten für Erhebungen, Prüfungen etc.
  + Spezialthemen für Verfahrensverantwortliche: Verfahrensbeschreibung, Auftragsverarbeitung, Datenschutzfolgenabschätzung, Privacy by design/default
  + Handlungsanweisungen für die interne Meldung von Datenpannen und zur Bearbeitung oder Weiterleitung von Anfragen bzgl. der Betroffenenrechte
  + Information zur hochschulinternen Beratung durch Datenschutzkoordinatoren und Datenschutzbeauftragten
* Die Datenschutzkoordinatoren und die oder der Datenschutzbeauftragte stehen auf Anfrage jederzeit für allgemeine und spezialthematische Beratung in Datenschutzfragen für alle Angehörigen und Mitglieder der Hochschule zur Verfügung.
* Die oder der Datenschutzbeauftragte ist Kontaktpunkt für betroffene Personen.
  + Veröffentlichung der Kontaktdaten der bzw. des Datenschutzbeauftragten auf der Internetseite sowie auf allen Informationsbögen gemäß Art. 13, 14 DS-GVO

## Strukturelle und organisatorische Sicherstellung der Erfüllung der Anforderungen an Auftragsverarbeitungen

Die Hochschule ist für alle Verarbeitungen personenbezogener Daten, bei denen sie die Mittel und Zwecke bestimmen kann, verantwortlich. Sie kann für die Erreichung des Zwecks personenbezogene Daten durch geeignete Auftragsverarbeiter verarbeiten lassen, wobei Auftragsverarbeiter gemäß Art. 28 Abs. 10 DS-GVO keine Zwecke oder Mittel der Verarbeitung bestimmen können dürfen[[2]](#footnote-2). Die Hochschule benötigt keine Rechtsgrundlage für die Weitergabe der personenbezogenen Daten an den Auftragsverarbeiter, da hierfür weiterhin die der Datenverarbeitung zugrundeliegende Rechtsgrundlage herangezogen werden kann und der Auftragsverarbeiter nicht als Dritter i. S. d. Art. 4 Nr. 10 DS-GVO zu sehen, sondern dem „Innenverhältnis“ der Hochschule hinzuzurechnen ist. Die Ermittlung des Vorliegens einer Auftragsverarbeitung bedarf eines gewissen Vorwissens im Datenschutz und wird den meisten fachlich Verantwortlichen nicht ohne Hilfestellung möglich sein. Eine entsprechende Handreichung sollte sich auf die eindeutigen Fälle beschränken und für die dazwischenliegenden schwierigen Fälle eine Prüfung durch den Datenschutzkoordinatorin / den Datenschutzkoordinator und ggf. weitergehend die Stabsstelle Datenschutzz vorgeben. Hierbei muss klargestellt werden, dass im Interesse der Hochschule ein sorgfältiger Umgang mit dem Thema Auftragsverarbeitung geboten ist, der dadurch hergestellt wird, indem alle Anforderungen und Grundsätze aus Art. 5 DS-GVO gewissenhaft erfüllt werden.

**Erforderliche Dokumente:**

* Handreichung für die Verantwortlichen und innen und -koordinatoren, wann eine Auftragsverarbeitung vorliegt und wer ggf. mit einzubeziehen ist

Der Hochschule als Verantwortliche der Verarbeitung wird durch Art. 28 Abs. 1 DS-GVO auferlegt, vor Auftragsvergabe eine Prüfung der Eignung des Auftragsverarbeiters durchzuführen. Die Prüfung zielt darauf ab, ob der Auftragsverarbeiter hinreichende Garantien für geeignete technische und organisatorische Maßnahmen bietet, damit die Verarbeitung die datenschutzrechtlichen Vorgaben einhält und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

**Erforderliche Dokumente:**

* Richtlinien (ggf. mit Checkliste) für die Verantwortlichen bei der Auswahl von Auftragsverarbeitern

Die Verarbeitung durch den Auftragsverarbeiter erfolgt auf Grundlage eines Vertrags[[3]](#footnote-3), der den Auftragsverarbeiter an die Hochschule bindet und in dem die Verarbeitung festgelegt wird. Alternativ kann der Vertrag gemäß Art. 28 Abs. 6 DS-GVO auf den Standardvertragsklauseln gemäß Abs. 7, 8 beruhen.

**Erforderliche Dokumente:**

* Vorlage Vertrag zur Auftragsverarbeitung gemäß gesetzlicher Anforderungen

Die Festlegung der Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung erfolgt gemäß Art. 28 Abs. 3 DS-GVO über Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen und die Pflichten und Rechte der Hochschule. Die weiteren elementaren Punkte, die für eine Auftragsverarbeitung vertraglich fixiert werden müssen, sind:

1. **Verarbeitung nur auf dokumentierte Weisung der Hochschule**: Der Auftragsverarbeiter wird vertraglich verpflichtet, die übermittelten personenbezogenen Daten nur entsprechend der Weisungen der Hochschule zu verarbeiten.

Sollte der Auftragnehmer einer rechtlichen Verpflichtung zur Verarbeitung unterliegen, so ist er gesetzlich verpflichtet, dies der Hochschule vor der Verarbeitung mitzuteilen.

1. **Verpflichtung der beschäftigten Mitarbeiter zur Wahrung der Vertraulichkeit**: Der Auftragnehmer wird verpflichtet, nur diejenigen Mitarbeiter, die sich zur Wahrung der Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, mit der Verarbeitung der personenbezogenen Daten, die Gegenstand dieses Vertrags sind, zu beschäftigen. Es folgt hieraus nicht, dass der Auftragsverarbeiter alle seine Mitarbeiter verpflichten muss; der Auftragsverarbeiter darf nur diejenigen Mitarbeiter mit der Verarbeitung betrauen, die sich verpflichtet haben.
2. **Ergreifung erforderlicher technischer und organisatorischer Maßnahmen**: Der Auftragnehmer wird verpflichtet, technische und organisatorische Maßnahmen anzuwenden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Vertrag sollte hierzu ein Mindestmaß an technischen und organisatorischen Maßnahmen vorsehen, die der Auftragsverarbeiter erfüllen muss. Die Maßnahmen werden nicht direkt durch den Verantwortlichen vorgegeben, aber gemäß Punkt h) sowie gem. Art. 5 DS-GVO und gem. dem Standard-Datenschutzmodell (SDM) muss die Dokumentation und der Zugang zur Überprüfung der Hochschule zur Verfügung gestellt werden, damit diese die Einhaltung der Anforderungen überprüfen und die Überprüfung nachweisen kann.
3. **Einhaltung der Anforderungen an Unterauftragsverarbeitungen**: Es wird vertraglich festgehalten, ob und wie der Auftragnehmer weitere Auftragnehmer in Anspruch nehmen kann und auf welchem Wege die Hochschule informiert werden muss. Die Hochschule bleibt nur für die Überprüfung ihrer direkten Auftragnehmer verantwortlich, da der Auftragnehmer für die Unterauftragsverarbeitungsverhältnisse gemäß Art. 28 Abs. 4 DS-GVO die Pflichten und insbesondere die Haftung des Verantwortlichen übernimmt.
4. **Unterstützung der Hochschule (Auftraggeber) bei Gewährleistung der Betroffenenrechte**: Es muss vertraglich vereinbart werden, wie der Auftragsverarbeiter (und gemäß Punkt d) auch mögliche Unterauftragsverarbeiter) die Hochschule bei der Gewährleistung der Betroffenenrechte unterstützt. Wichtige Themen sind dabei Ansprechpartner, die technischen Mittel zur Übermittlung von Anfrage und Antwort sowie die Einhaltung von Fristen und Wahrung der Vertraulichkeit.
5. **Unterstützung der Hochschule (Auftraggeber) bei Datenpannen und Datenschutzfolgenabschätzung**: Der Auftragnehmer muss der Hochschule Datenpannen gemäß Art. 33 Abs. 2 DS-GVO unverzüglich melden und auch die weiteren, benötigten Informationen zur Erfüllung der Aufgaben der Hochschule als Verantwortliche der Verarbeitung personenbezogener Daten aus den Art. 33, 34 DS-GVO liefern. Ebenso muss der Auftragnehmer Überprüfungen der Verarbeitung durch die Hochschule gemäß Art. 35 Abs. 11 DS-GVO unterstützen.
6. **Löschung oder Rückgabe personenbezogener Daten bei Ende des Auftragsverhältnisses**: Die Einhaltung der Grundsätze beinhalten auch die Löschung personenbezogener Daten nach Ablauf der Erforderlichkeit. Da der Zweck der Auftragsverarbeitung mit dem Ende des Vertrags erbracht ist, ist daher auch eine Löschung bzw. Rückgabe der Daten an die Hochschule zur Einhaltung der Anforderungen gemäß DS-GVO erforderlich und muss vertraglich festgehalten werden.
7. **Zusammenarbeit zur Einhaltung der Anforderungen**:

**Zurverfügungstellung aller erforderlichen Informationen zur Einhaltung der Anforderungen**: Es muss vertraglich fixiert werden, dass der Auftragnehmer – auf Anfrage – die erforderlichen Informationen zur Verfügung stellt, aus denen die Hochschule schließen kann, dass die Verarbeitung die Anforderungen der Verordnung erfüllt. Für den Fall der Weigerung, der nicht rechtzeitigen Bereitstellung oder der Nichtbereitstellung dieser Informationen sollten angemessene Vertragsstrafen festgelegt werden.

**Überprüfungen ermöglicht**: Ebenso muss vertraglich fixiert werden, dass der Auftragnehmer Überprüfungen durch die Hochschule oder einen von der Hochschule benannten Prüfer ermöglicht und unterstützt.

**Hinweis auf Verstoß einer Weisung gegen Datenschutzbestimmungen**: Der Auftragnehmer ist gesetzlich durch Art. 28 Abs. 3 Unterabsatz 2 DS-GVO verpflichtet, Weisungen, die seiner Meinung nach gegen Datenschutzbestimmungen verstoßen, der Hochschule zu melden. Die Meldewege hierfür müssen vertraglich festgelegt werden.

## Strukturelle und organisatorische Sicherstellung der Erfüllung der Anforderungen bei einer Übermittlung von personenbezogenen Daten in Drittstaaten

Bei einer geplanten Übermittlung von personenbezogenen Daten in einen Drittstaat (Land außerhalb der EU) ist neben der rechtlichen Zulässigkeit der Verarbeitung die Zulässigkeit der Übermittlung in den jeweiligen Drittstaat zu prüfen. Da in dem Drittstaat die DS-GVO nicht gilt muss sichergestellt sein, dass ein der DS-GVO vergleichbares Schutzniveau bei der Stelle in dem Drittstaat existiert.

Art. 44 DS-GVO enthält diesbezüglich einen Schutz, der die Untergrabung des Schutzniveaus verhindern soll. Demnach gelten die Bestimmungen der DS-GVO auch dann, wenn die Daten in einen ersten Drittstaat nur für die Durchleitung in einen anderen Drittstaat übermittelt werden, in dem die Daten dann weiterverarbeitet werden sollen. Durch ein solches Vorgehen lässt sich somit die DS-GVO als mögliches Hindernis für eine Übermittlung in einen Drittstaat nicht abschütteln.

Ob eine Prüfung für eine zulässige Drittstaatenübermittlung durchgeführt werden muss, stellt sich schon im Rahmen der Aufstellung des jeweiligen Verzeichnisses der Verarbeitung heraus. Bereits in dem Ersterhebungsfragebogen wird die Frage danach gestellt, ob personenbezogene Daten in einen Staat außerhalb der EU übermittelt werden. Trifft dies zu, so ist die fachlich verantwortliche Stelle für die Prüfung und Sicherstellung einer zulässigen Drittstaatenübermittlung verantwortlich. Die fachlich verantwortliche Stelle wird hierbei durch ihre Datenschutzkoordinatorin bzw. ihren Datenschutzkoordinator und durch die Stabsstelle Datenschutz unterstützt.

**Erforderliche Dokumente:**

* Handreichung zur Drittstaatenübermittlung aus der hervorgeht, was in diesem Fall zu tun ist.

Eine Übermittlung in Drittstaaten ist unter den folgenden Voraussetzungen zulässig:

### Angemessenheitsbeschluss

Eine Übermittlung ist oft unproblematisch möglich, wenn ein Angemessenheitsbeschluss der EU-Kommission existiert. In diesen Fällen hat die Kommission beschlossen, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Es bedarf dann keiner besonderen Genehmigung. In den einfach gelagerten Fällen, in denen sich ein Angemessenheitsbeschluss gleich auf ein ganzes Drittland bezieht (z. B. Schweiz oder Kanada), kann eine Handreichung erstellt werden, auf Basis derer die Prüfung alleine durch den fachlich Verantwortlichen ggf. in Zusammenarbeit mit dem Datenschutzkoordinator erfolgen kann.

**Erforderliche Dokumente:**

* Handreichung für fachlich Verantwortliche über die Anwendung von Angemessenheitsbeschlüssen auf die Übermittlung in Drittstaaten.

### Einwilligung des Betroffenen

Nach Art. 49 Abs. 1 Buchst. a) DS-GVO ist im Einzelfall eine Übermittlung auch dann zulässig, wenn die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt hat, nachdem sie über mögliche Risiken unterrichtet wurde. Hier wird eine Vorlage für Einwilligungen in unterschiedlichen Fallkonstellationen (Forschungsdaten, Übermittlung an Kooperationshochschule) zur Verfügung gestellt, mit Hilfe derer die fachlich Verantwortlichen ggf. zusammen mit der Datenschutzkoordinatorin / dem Datenschutzkoordinator selbst die Voraussetzungen für die zulässige Übermittlung schaffen können. Bei einer Einwilligung von Beschäftigten und in manchen Fällen auch von Studierenden ist der Grundsatz der Freiwilligkeit einer Einwilligung besonders zu prüfen, da hier jeweils ein Abhängigkeitsverhältnis zur Hochschule besteht.

**Erforderliche Dokumente:**

* Vorlagen für Einwilligungen durch Betroffene in Drittstaatenübermittlungen

### Angemessenheitsbeschlüsse mit Prüfungsbedarf, Übermittlungen vorbehaltlich geeigneter Garantien, weitere Ausnahmen im Einzelfall nach Art. 49

In allen weiteren Fällen besteht ein erweiterter rechtlicher Prüfungsbedarf, bevor die Datenübermittlung aufgenommen werden darf. Diese Fälle müssen im Rahmen der Ersterhebung der Verarbeitung und mit Hilfe der Handreichung ermittelt und an die Stabsstelle Datenschutz oder das Rechtsreferat/die Rechtsabteilung zur Prüfung und weiteren Entscheidung weitergegeben werden. Die Übermittlung darf erst nach einer verbindlichen Entscheidung von dort aufgenommen werden.

### Bestandsverarbeitungen

Dies betrifft Bestandsfälle, in denen bereits Daten an Drittstaaten übermittelt werden, bei denen aber noch keine Prüfung der Zulässigkeit der Drittstaatenübermittlung vorgenommen wurde. Bei diesen Verarbeitungen wird entsprechend dem Vorgehen bei neuen Verarbeitungen vorgegangen. Ergibt sich aus dem Ersterhebungsbogen oder aus dem bestehenden Verfahrensverzeichnis (nach alter Rechtslage) eine Übermittlung von Daten in einen Drittstaat, so ist die Prüfung entsprechend derer von neuen Verarbeitungen vorzunehmen. Die interne Verantwortung für die Rechtmäßigkeit der Übermittlung in einen Drittstaat liegt auch hier bei der fachlich verantwortlichen Stelle.

## Datenschutz-Folgenabschätzung (DSFA)

Eine Datenschutz-Folgenabschätzung (DSFA) ist durchzuführen, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Regelbeispiele für die Erforderlichkeit einer DSFA finden sich in Art. 35 Abs. 3 DS-GVO. Diese sind nicht abschließend, sondern nur Beispiele, bei denen eine DSFA erforderlich ist.

Das hohe Risiko einer Verarbeitung kann sich gemäß Art. 35 Abs. 1 DS-GVO aufgrund der Verwendung einer neuen Technologie, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ergeben. Das Vorliegen eines hohen Risikos wird mit Hilfe der Schwellwertanalyse festgestellt. Kriterien für die Prüfung ergeben sich neben Art. 35 Abs. 1 und 3 DS-GVO auch aus den Positivlisten, die gemäß Art. 35 Abs. 4 DS-GVO durch die Aufsichtsbehörden zu veröffentlichen sind. Ergibt die Schwellwertanalyse ein hohes Risiko, ist eine Datenschutz-Folgeabschätzung durchzuführen. Anhand der festgestellten Risiken sind geeignete Abhilfemaßnahmen zum Ausschluss oder zur Eindämmung des Risikos festzulegen und umzusetzen. Gelingt dies nicht, muss vor Aufnahme der Verarbeitung die zuständige Datenschutzaufsichtsbehörde konsultiert werden. Diese kann weitere Maßnahmen oder Beschränkungen der Verarbeitung vorschlagen, aber auch von ihren aufsichtsrechtlichen Befugnissen Gebrauch machen, bis hin zur Untersagung der geplanten Verarbeitung.

Die Verantwortung innerhalb der Hochschule obliegt der fachlich verantwortlichen Stelle. Diese hat mit Unterstützung der Datenschutzkoordinatorin / des Datenschutzkoordinators eine Schwellwertanalyse zu veranlassen und diese durch richtige und vollständige Angaben zu unterstützen. Die Schwellwertanalyse und die Datenschutz-Folgeabschätzung werden fachlich durch die Stabsstelle Datenschutz durchgeführt. Die oder der Datenschutzbeauftragte ist beratend hinzuzuziehen. Die Festlegung von Maßnahmen erfolgt verbindlich durch die Stabsstelle Datenschutz. Ebenso entscheidet die Stabsstelle Datenschutz verbindlich über eine vorherige Konsultation der zuständigen Datenschutzaufsichtsbehörde nach Art. 36 DS-GVO.

# Verarbeitungsbezogene Gewährleistung der Anforderungen

Für die verarbeitungsbezogene Gewährleistung der materiellen Anforderungen wird das Prüfschema des Standard-Datenschutzmodells herangezogen. Im Folgenden zeigt sich, dass sich die Anforderungen aus Art. 5 Abs. 1 DS-GVO mit deren Konkretisierungen in weiteren Rechtsnormen abbilden lassen. Die verarbeitungsbezogenen Angaben ermöglichen die Aufnahme der jeweiligen Verarbeitung in das Verzeichnis von Verarbeitungen.

## Verantwortliche Stelle

Verantwortliche Stelle ist die für die Verarbeitung verantwortliche juristische Person. Verantwortliche Stelle für alle für die Hochschule vorgenommenen Verarbeitungen ist die Hochschule.

## Zweck der Verarbeitung

Welche Zwecke werden mit der Verarbeitung von personenbezogenen Daten verfolgt? Die Prüfung der Rechtmäßigkeit erfolgt anhand der jeweils mit der Verarbeitung verfolgten Zwecke. Es sind somit stets alle Zwecke vollständig zu ermitteln und für weitere Prüfungen zu dokumentieren, damit die Hochschule ihren Nachweispflichten nachkommen kann.

## Rechtsgrundlage (Art. 5 Abs. 1 a) a.)

Für die Verarbeitung personenbezogener Daten ist in jedem Fall eine Rechtsgrundlage erforderlich, die den konkret verfolgten Zweck vollständig abdeckt. Es ist daher vor Aufnahme einer Verarbeitung von personenbezogenen Daten stets zu prüfen, ob eine Rechtsgrundlage besteht, die eine Verarbeitung dieser personenbezogenen Daten, dieser Betroffenen zu diesem Zweck erlaubt:

* Gesetzliche Rechtsgrundlage
* Einwilligung
* Auftragsverarbeitung
* Übermittlung in ein Drittland

## Gewährleistungsziel Datensparsamkeit (Art. 5 Abs. 1 a) a.)

Es dürfen nur die für den jeweiligen Verarbeitungszweck erforderlichen personenbezogenen Daten verarbeitet werden. Die Prüfung erfolgt nach den Kriterien des Standard-Datenschutzmodells (SDM) auf das diesbezüglich verwiesen wird.

## Gewährleistungsziel Transparenz (Art. 5 Abs. 1 a) b., c. und d.)

Die Verarbeitung von personenbezogenen Daten muss den Anforderungen der Transparenz genügen. Wichtig ist in diesem Zusammenhang insbesondere die Erfüllung der verarbeitungsbezogenen Informationspflichten. Die Prüfung erfolgt nach den Kriterien des Standard-Datenschutzmodells (SDM) auf das diesbezüglich verwiesen wird.

## Gewährleistungsziel Verfügbarkeit (Art. 5 Abs. 1 f))

**Gemäß Informationssicherheitsmanagement unter Berücksichtigung besonderer Datenschutzaspekte aus dem SDM**

In diesem Bereich besteht die inhaltliche Verzahnung mit der Informationssicherheit, so dass weitreichend Synergien genutzt werden können. Konflikte können sich in Bezug auf Löschfristen ergeben, wenn diese nicht explizit durch ein Gesetz festgelegt sind. Hier ist gegebenenfalls ein Aushandeln im Einzelfall mit entsprechender Dokumentation erforderlich.

* Gegebenenfalls Unterstützung durch ein geeignetes Tool

## Gewährleistungsziel Integrität (Art. 5 Abs. 1 d) und f))

**Gemäß Informationssicherheitsmanagement unter Berücksichtigung besonderer Datenschutzaspekte aus dem SDM**

Auch hier besteht die inhaltliche Verzahnung mit der Informationssicherheit, so dass weitreichend Synergien genutzt werden können. Konflikte können sich in Bezug auf die Löschung, Pseudonymisierung und Anonymisierung von personenbezogenen Daten ergeben, die gegebenenfalls auch für Sicherheitszwecke relevant sein können. Hier ist gegebenenfalls ein Aushandeln im Einzelfall mit entsprechender Dokumentation erforderlich.

* Gegebenenfalls Unterstützung durch ein geeignetes Tool

## Gewährleistungsziel Vertraulichkeit (Art. 5 Abs. 1 f))

**Gemäß Informationssicherheitsmanagement unter Berücksichtigung besonderer Datenschutzaspekte aus dem SDM**

Auch hier besteht die inhaltliche Verzahnung mit der Informationssicherheit, so dass weitreichend Synergien genutzt werden können. Konflikte können sich in Bezug auf die Vertraulichkeit bezüglich Kenntnisnahmen interner Personen ergeben. Dies wird vor allem den Bereich Protokollierung und Auswertung von Protokollen betreffen.

* Gegebenenfalls Unterstützung durch ein geeignetes Tool

## Gewährleistungsziel Nichtverkettbarkeit (Art. 5 Abs. 1 b), c) und e))

Die Nichtverkettbarkeit ist wesentlich für einen wirksamen Grundrechtsschutz, indem durch eine aufgabengerechte Trennung von Verarbeitungszwecken und einer entsprechenden Gestaltung von Zugriffsrechten ein umfassend auswertbares Bild einer betroffenen Person zumindest deutlich erschwert wird. Wichtige Maßnahmen sind in diesem Zusammenhang auch: Anonymisierung und Pseudonymisierung von personenbezogenen Daten. Die Prüfung erfolgt nach den Kriterien des Standard-Datenschutzmodells (SDM) auf das diesbezüglich verwiesen wird.

## Gewährleistungsziel Intervenierbarkeit (Art. 5 Abs. 1 d) und e))

Die Intervenierbarkeit soll die Möglichkeit der Einflussnahme des Betroffenen auf die Verarbeitung seiner personenbezogenen Daten gewährleisten. Maßnahmen zur operativen Unterstützung der Betroffenenrechte finden sich in Art. 12 bis 23 DS-GVO. Die Prüfung erfolgt nach den Kriterien des Standard-Datenschutzmodells (SDM), auf das diesbezüglich verwiesen wird.

**Hinweis zum Standard-Datenschutzmodell (SDM):**

Die verfahrensbezogene Gewährleistung der materiellen Anforderungen muss nicht nach dem Prüfschema des SDM erfolgen. Die dortigen Prüfpunkte lassen sich systematisch auch anderweitig abbilden. Allerdings würde dies die Anwendung des Schutzmaßnahmen-Referenzkatalog (Anhang A zum SDM-Handbuch und bisher nicht verfügbar) erschweren.

# IV. Weiterentwicklung des Ansatzes zum Datenschutzmanagement

Damit sich die Implementierung von Maßnahmen nicht in einem einmaligen Tun erschöpfen und stets an neue organisatorische und technische Gegebenheiten angepasst werden, muss ein System zur stetigen Verbesserung implementiert werden. Dies ist insbesondere auch für die Gewährleistung der Nachweispflichten aus der DS-GVO erforderlich. Folgerichtig findet sich das Datenschutzmanagement auch im SDM-Baustein 80 wieder, auf welchen hier verwiesen wird. Als Ansatz für ein Managementsystem hat sich der PDCA-Zyklus (Demingkreis) bewährt. PDCA steht hierbei für Plan-Do-Check-Act:

## Plan: Planungsphase

In der Planungsphase müssen die Verarbeitungen mit personenbezogenen Daten identifiziert und dokumentiert werden. Die Dokumentation bildet die Basis für die Schwellwertanalyse um den Schutzbedarf festzustellen. Bei bekanntem Schutzbedarf lassen sich angemessene Maßnahmen zum Schutz der Verarbeitung der personenbezogenen Daten im Sinne des Art. 32 DS-GVO bestimmen und in die Umsetzungsplanung integrieren.

## Do: Umsetzungsphase

Die in der Planungsphase entwickelten Konzepte und Maßnahmen werden umgesetzt. Dies erfordert ein planvolles und strukturiertes Vorgehen, an dem alle maßgeblichen Akteure angemessen beteiligt werden müssen. Umsetzung und Verantwortlichkeiten müssen dokumentiert werden, damit die tatsächliche Umsetzung nachgewiesen werden kann.

## Check: Überprüfungsphase

Die Umsetzung von Konzepten und Maßnahmen und die Konzepte selbst müssen laufend auf ihre Wirksamkeit überprüft werden. Dabei stellen sich im Wesentlichen zwei Herausforderungen:

1. Die Wirksamkeit kann durch nachträgliche Änderungen oder Erweiterungen beeinträchtigt werden. Bei diesbezüglichen Veränderungen muss das Verzeichnis der Verarbeitungen angepasst werden und eine anlassbezogene Prüfung der Maßnahmen und Konzepte angestoßen werden. Neben der anlassbezogenen Überprüfung sollte zudem eine zeitlich regelmäßig erfolgende Überprüfung stattfinden, um unbemerkte allmähliche Veränderungen an Verarbeitungen mit Relevanz für die Konzepte und Maßnahmen aufdecken zu können. Für eine solche regelmäßige Überprüfung gibt es keine feste gesetzliche Frist. Als Orientierung kann aber aus dem Bereich der Informationssicherheit der § 8a Abs. 3 BSIG dienen, der eine Überprüfung von Maßnahmen mindestens alle zwei Jahre vorsieht. Entsprechend werden die fachlich Verantwortlichen alle zwei Jahre aufgefordert, die unveränderte Verarbeitung zu bestätigen oder zwischenzeitliche Änderungen zum Verzeichnis der Verarbeitungen zu melden.
2. Weiterhin können Änderungen beim Stand der Technik dazu führen, dass die ursprünglich ergriffenen Sicherheitsmaßnahmen nicht mehr als angemessen angesehen werden können. Auch hier sind anlassbezogene Prüfungen vorzunehmen, wenn bekannt wird, dass bestimmte bisher als sicher geltende Maßnahmen nicht mehr als ausreichend anzusehen sind (z. B. ein Verschlüsselungsalgorithmus ist nicht mehr sicher). Zur Sicherstellung des Stands der Technik müssen auch hier regelmäßige Überprüfungen erfolgen. Mangels einer gesetzlich vorgeschriebenen Frist, sollte auch hier die Frist aus § 8a Abs. 3 BSIG von zwei Jahren als Orientierung herangezogen werden.

Ebenso wie die Umsetzung muss auch die Überprüfung zur Erfüllung der Nachweispflichten dokumentiert werden.

## Act: Anpassungsphase

In der Anpassungsphase werden die in der Überprüfungsphase festgestellten Mängel bzw. der festgestellte Optimierungsbedarf umgesetzt. Auch hier müssen Umsetzung und Verantwortlichkeiten zur Erfüllung der Nachweispflichten dokumentiert werden.

# V. Umgang mit Anfragen von Sicherheits- und Strafverfolgungsbehörden

Zu unterscheiden ist zunächst zwischen Anfragen von Sicherheits- und Strafverfolgungsbehörden. Anfragen von Sicherheitsbehörden dienen der Abwehr einer möglichen Gefahr, während Anfragen der Strafverfolgungsbehörden dazu dienen, eine bereits erfolgte Straftat aufzuklären. Aufgrund dieser unterschiedlichen Aufgaben handeln die Behörden auf Grundlage unterschiedlicher Befugnisnormen. Die Befugnisnormen begründen eine rechtliche Pflicht der Hochschule zur Auskunfterteilung. Soweit personenbezogene Daten betroffen sind, ergibt sich die gesetzliche Erlaubnis zur Verarbeitung und Übermittlung zur Erfüllung dieser Pflicht aus Art. 6 Abs. 1 lit. c DS-GVO. Die Erlaubnis besteht jedoch nur soweit die Pflicht zur Auskunfterteilung besteht. Die Hochschule muss somit organisatorisch sicherstellen, dass eine Auskunft nur im Rahmen einer bestehenden Pflicht erfolgt und, dass hierbei die Betroffenenrechte gewahrt werden.

## Anfragen von Strafverfolgungsbehörden

Die Strafverfolgungsbehörden stellen im Rahmen ihrer Ermittlungen in der Regel Anfragen nach den folgenden Befugnisnormen:

* § 161 Abs. 1 Strafprozessordnung (StPO): Demnach ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen.
* §§ 100a, 100b StPO: Erlaubt die inhaltliche Überwachung der Kommunikation unter hohen Anforderungen. Insbesondere muss eine schwere Katalogstraftat nach § 100a Abs. 2 StPO vorliegen. Formell muss ein richterlicher Beschluss vorliegen. Bei Gefahr in Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Diese muss innerhalb von drei Werktagen gerichtlich betätigt werden.
* § 100g StPO: Erlaubt die Auskunft über Verkehrsdaten und setzt ebenfalls einen richterlichen Beschluss und eine Katalogstraftat nach § 100a Abs. 2 StPO voraus oder den Verdacht, dass die Straftat mittels Telekommunikation begangen wurde und die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Verkehrsdaten beinhalten nicht die Inhalte der Kommunikation aber deren Begleitumstände, aus denen sich Kommunikationspartner, Dauer der Kommunikation und ggf. Standorte ableiten lassen. Bei Gefahr in Verzug kann unter den gleichen Bedingungen wie bei § 100a StPO die Anordnung auch durch die Staatsanwaltschaft erfolgen.
* § 100j StPO i. V. m. § 113 TKG: Erlaubt die Einholung der Auskunft über den Anschlussinhaber anhand der zugeordneten IP-Adresse und einem Zeitstempel und Auskünfte über Zugangsdaten. Bei Auskünften über Zugangsdaten ist ein richterlicher Beschluss erforderlich. Bei Gefahr im Verzug kann auch hier die Anordnung durch die Staatsanwaltschaft oder ihre Ermittlungspersonen erfolgen.

Bei den Befugnissen durch die Staatsanwaltschaft ist zu beachten, dass diese auch durch Polizeibeamte und Kriminalbeamte als Ermittlungspersonen der Staatsanwaltschaft gemäß § 152 GVG i. V. m. der Verordnung über Ermittlungspersonen der Staatsanwaltschaft (NRW) ausgeübt werden können. Es tritt einem somit nicht unbedingt ein Staatsanwalt/eine Staatsanwältin in Robe gegenüber, sondern meist ein Polizeibeamter/eine Polizeibeamtin.

Ausländische Strafverfolgungsbehörden treten nicht direkt in Erscheinung sondern über die inländischen Strafverfolgungsbehörden über Rechtshilfeersuchen.

## Sicherheitsbehörden und Geheimdienste

Die Landespolizeigesetze enthalten Befugnisse der Sicherheitsbehörden, Auskünfte zur Gefahrenabwehr zu verlangen. Dies schließt auch personenbezogene Daten mit ein:

Insbesondere im Polizeigesetz des Landes NRW finden sich die folgenden Rechtsgrundlagen:

* § 9 PolG: Befragung und Auskunftspflicht
* § 11 PolG: Erhebung von Personaldaten zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen
* § 20a PolG: Abfrage von Telekommunikations- und Telemediendaten
* § 20c PolG: Datenerhebung durch die Überwachung der laufenden Telekommunikation

Darüber hinaus können auch die Geheimdienste zu ihrer Aufgabenerfüllung Auskünfte verlangen. Folgende Befugnisse bestehen:

* § 8a Bundesverfassungsschutzgesetz
* § 7c Gesetz über den Verfassungsschutz in Nordrhein-Westfalen
* § 5 BND-Gesetz

## Prozessuale Sicherstellung der Zulässigkeit der Verarbeitung

Die Verarbeitung und Übermittlung personenbezogener Daten im Rahmen eines behördlichen Auskunftsverlangens ist gemäß Art. 6 Abs. 1 lit. c DS-GVO zulässig, soweit die damit verbundene Verarbeitung zur Erfüllung einer Rechtspflicht der Hochschule erforderlich ist. Die Rechtspflicht ergibt sich aus der jeweiligen Befugnisnorm der anfragenden Behörde, die die Hochschule zur Auskunfterteilung oder zur Zurverfügungstellung von Informationen verpflichtet. Darüber hinausgehende Verarbeitungen sind nicht zulässig, weshalb Bearbeitungsprozesse eingerichtet werden müssen, die die Zulässigkeit der Verarbeitung prozessual sicherstellen.

Es ist bei der Bearbeitung von Anfragen oder Aufforderungen von Strafverfolgungsbehörden auf drei Phasen abzustellen:

1. Erhalt der Anfrage/Aufforderung
2. Bearbeitung
3. Auskunfterteilung/Zurverfügungstellung der Informationen/Duldung von Maßnahmen

### Erhalt der Anfrage/Aufforderung

Die initiale Geltendmachung der Befugnisse kann in verschiedenen Formen erfolgen. Es kann sich um eine Anfrage per Telefon, Fax oder E-Mail handeln. Es kann aber auch sein, dass die Beamten direkt vor Ort Auskunft die Zurverfügungstellung von Informationen oder die Duldung von Maßnahmen verlangen. Vorkehrungen durch die Hochschule müssen sich demnach danach richten, an welchen Stellen diese Anfragen/Aufforderungen ankommen können. Die betreffenden Beschäftigten werden sensibilisiert, welche Aktionen im Falle einer Anfrage/Aufforderung nötig sind. An den folgenden Stellen besteht allgemein eine erhöhte Wahrscheinlichkeit:

* Kontaktdaten der Hochschule im Impressum oder in der Datenschutzerklärung der Webseite (Netzrecherchen der Behörden)
* Abuse-Kontakt bei der TLD-Registrierungsstelle für den eigenen Domain-/IP-Adressbereich
* Hausmeister, Pförtner, Sekretariate bei persönlichem Erscheinen

Hierbei ist organisatorisch folgendes zu beachten:

* Grundsätzlich sind die betreffenden Personen zur Entgegen- und Aufnahme der Anfragen/Aufforderungen befugt.
* Aufnahme des Sachverhalts: Wer, von welcher Behörde möchte was auf welcher rechtlichen Grundlage? Bei Bestehen eines richterlichen Beschlusses sollte eine Kopie des Beschlusses verlangt bzw. angefertigt werden. Bei persönlichem Erscheinen sollte das Vorzeigen des Dienstausweises verlangt und bei Zweifeln bei der Dienststelle nachgefragt werden.
* Meldewege und Beteiligungspflichten: Wer muss unverzüglich informiert und nach Möglichkeit hinzugezogen werden?
* Bei Duldung von Maßnahmen (z. B. Durchsuchung, Beschlagnahme): Nach Möglichkeit sollten Zeugen hinzugezogen werden. Sollte dies nicht möglich sein, sollte ein Protokoll zur Gedächtnisstütze für eine mögliche spätere Aussage erstellt werden. Aktiver Widerstand gegen die Maßnahmen von echten Beamten muss unterlassen werden, da ansonsten eine Strafbarkeit wegen Widerstands gegen Vollstreckungsbeamte droht.
* In allen anderen Fällen: Klärung, an wen die Anfrage/Aufforderung zur weiteren Bearbeitung weitergeleitet werden soll. In der Regel wird eine Weiterleitung an das Justiziariat zur weiteren Bearbeitung sinnvoll sein, um die Verarbeitung personenbezogener Daten im rechtlich zulässigen Rahmen sicherzustellen.

### Bearbeitung

Nach der Weitergabe an die intern zuständige Stelle (z. B. Justiziariat), erfolgt die weitere Bearbeitung:

* Prüfung der Rechtsmäßigkeit und Validität der Anfrage/Aufforderung: Insbesondere muss hier festgestellt werden, ob die Hochschule der Rechtsgrundlage auf der die Anfrage/Aufforderung basiert wirklich unterliegt und ob Sie dieser auch folgen muss.
* Formelle Prüfung eines Beschlusses: Hier erfolgt die Überprüfung des Beschlusses auf offenkundige Fehler (z. B. der Beschluss bezieht sich gar nicht auf die Hochschule). Eine materiellrechtliche Prüfung eines Beschlusses wird jedoch nicht verlangt und ist den Gerichten vorbehalten. Bis zu einer gerichtlichen Aufhebung eines Beschlusses muss dieser im Zweifel umgesetzt werden, wobei die Behörde die Verantwortung trägt. Allerdings sollte die Hochschule die Behörde auf diese Fehler hinweisen.
* Zusammenstellung der Informationen: Die für die Auskunfterteilung notwendigen Informationen müssen eingeholt und zusammengestellt werden. Hier ist es notwendig den Kreis der mit der Anfrage Betrauten so gering wie möglich zu halten, um zum einen die Ermittlungen nicht zu gefährden, zum anderen aber auch den Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen (insbesondere wenn die Ermittlungen zu keiner Anklage o.Ä. führen) zu minimieren.

### Auskunfterteilung /Zurverfügungstellung der Informationen /Duldung von Maßnahmen

Es muss innerhalb der Hochschule festgelegt werden, von welcher Stelle die Auskunft erteilt wird. Dies kann z. B. das Justiziariat sein, das die Anfrage bereits bearbeitet hat. Folgendes ist hierbei zu beachten:

* Sicherstellung der Identität: Vor Erteilung einer Auskunft muss die Identität der anfragenden Behörde sichergestellt werden. Briefköpfe und E-Mail-Absender können mit digitalen Mitteln gefälscht werden. Ein Anruf bei der offiziellen Behördennummer kann hier Klarheit schaffen. Erfolgt die Aufforderung telefonisch, sollte auch in Eilfällen auf keinen Fall ohne einen verifizierenden Rückruf unter einer vorher geprüften Nummer eine Auskunft erteilt werden.
* Zusammenstellung der Auskunft: Bei der Zusammenstellung der Informationen sollte besonderes Augenmerk darauf gelegt werden, dass nur Informationen gesammelt bzw. übermittelt werden, welche eindeutig von der Anfrage erfasst sind. Es muss somit darauf geachtet werden, dass die Anfrage nicht übererfüllt wird.
* Weiterhin muss vor Übermittlung der Informationen/Dokumente an die Strafverfolgungsbehörde geprüft werden, ob ggf. Daten unbeteiligter Dritter in den Dokumenten vorliegen und diese ggf. entfernt werden müssen.
* Die Führung einer Dokumentation ist auch hier von äußerster Wichtigkeit und Unterlagen bzw. Korrespondenz sollten aufgrund ihrer Sensitivität gesondert verwahrt werden.

Information der / des Betroffenen: Bei der Eröffnung eines Verfahrens kann gegebenenfalls davon ausgegangen werden, dass der/die Betroffene im Sinne des Art. 15 Abs. 5 lit. a DS-GVO bereits über die Informationen verfügt. Sollte dies nicht der Fall sein, ist zu beachten, dass gemäß § 11 Abs. 2 DSG NRW eine Information nur mit Zustimmung der betreffenden Stelle (Ermittlungs- oder Polizeibehörde) gegeben werden darf. Gegebenenfalls wird diese selbst die betroffene / den Betroffenen informieren.

### Zusammenfassung von Kernaktivitäten

Allgemein:

* Implementierung eines Verfahrens und insbesondere einer Bearbeitungshierarchie
  + Information an alle Mitarbeitende in Kontaktpositionen (nach außen) über den weiteren Umgang mit solchen Anfragen/Aufforderungen

und

* + Schulung/Weisung an Mitarbeitende keine Informationen ohne vorherige Rücksprache mit der Rechtsabteilung – insbesondere telefonisch – herauszugeben und wie sie sich zu verhalten haben, wenn eine vorherige Rücksprache nicht möglich ist.
  + Besonderes Augenmerk auf Dokumentation von Vorgehen und involvierten Personen (dies erhöht auch die Rechtssicherheit im Falle eines „Leaks“ für geheim zu haltende Ermittlungsverfahren)
  + Definieren eines spezifischen Personenkreises, welcher nur mit solchen sensiblen Sachverhalten betraut wird. Dies sollte zumindest Umfassen: Personen in Leitungspositionen, Datenschutzbeauftragte bzw. Datenschutzbeauftragter, Rechtsabteilung bzw. Leiterin / Leiter der Rechtsabteilung, besonders betraute Sachbearbeiterinnen / Sachbearbeiter (ggf. Erfahren im Umgang mit sensiblen Sachverhalten etc.)
  + Festlegung auf eine spezifischen Ansprechpartnerin / einen spezifischen Ansprechpartner für Strafverfolgungsbehörden, bei der/dem alle Informationen zusammenlaufen

**Verfasser:**

RA Herr Dr. Köcher, DFN-CERT GmbH als Berater

für das Projektteam DSMS (Andreas Brennecke, DSB Universität Paderborn, Anja Schmid, DSB Universität Bielefeld, Birgit Schmahlenberg, FH Bielefeld)

1. Neben der zentralen Internetseite der Hochschule werden auch Internetseiten von Fachbereichen, Lehrstühlen und Projekten mit diesem Abschnitt angesprochen. Die Darstellung erfolgt daher entsprechend angepasst und verallgemeinert. [↑](#footnote-ref-1)
2. Die Bestimmung technisch-organisatorische Mittel ist gemäß dem Working Paper 169 der Artikel-29 Gruppe innerhalb des durch die Hochschule gesteckten Rahmens möglich. Diese Einschätzung wird von der LDI NRW in Kurzpapier 13 unterstützt. [↑](#footnote-ref-2)
3. Neben einem Vertrag können auch andere bindende Rechtsinstrumente nach Unionsrecht oder Bundes- oder Landesrecht als Grundlage für ein Auftragsverarbeitungsverhältnis verwendet werden. [↑](#footnote-ref-3)