

Verkündungsblatt 17|2019

Ausgabedatum 03.12.2019

Inhaltsübersicht

A. Bekanntmachungen nach dem NHG

Änderung der Nr. 9 der Richtlinie der Leibniz Universität Hannover zur Erteilung und Vergütung von Lehraufträgen Seite 2

Wahlordnung der Studierendenschaft Seite 3

B. Bekanntmachungen nach § 78 Abs. 2 NPersVG

Dienstvereinbarung gemäß über die Einführung einer Inventarisierungssoftware (Inventory Tool) Seite 12

Dienstvereinbarung über den Betrieb des Forschungsinformationssystems Pure Seite 16

Dienstvereinbarung zur Einführung eines Systems zur elektronischen Probandenverwaltung Seite 21

Dienstvereinbarung über die Einführung und Anwendung des Veranstaltungsmanagementsystems „Antrago“ Seite 43

C. Hochschulinformationen

A. Bekanntmachungen nach dem NHG

Das Präsidium der Leibniz Universität Hannover hat in seiner Sitzung am 10.10.2019 die Änderung der Nr. 9 der Richtlinie der Leibniz Universität Hannover zur Erteilung und Vergütung von Lehraufträgen beschlossen. Die Änderung tritt in der nachstehenden Fassung am Tage ihrer Veröffentlichung im Verkündungsblatt der Gottfried Wilhelm Leibniz Universität Hannover in Kraft.

Änderung der Nr. 9 der Richtlinie der Leibniz Universität Hannover zur Erteilung und Vergütung von Lehraufträgen

9. Höhe der Vergütung

Die Vergütung für Lehraufgaben einer Lehrkraft für besondere Aufgaben des gehobenen Dienstes sollte bis zu 20 €, für Lehraufgaben einer Lehrkraft für besondere Aufgaben des höheren Dienstes bis zu 22 € und für Lehraufgaben einer Professorin oder eines Professors bis zu 37 € je Einzelstunde betragen.

Hat der Lehrauftrag eine besondere Bedeutung oder ist er mit einer besonderen Belastung verbunden, kann der oder dem Lehrbeauftragten eine Einzelstundenvergütung von bis zu 60 € gezahlt werden.

Bei der Festlegung der Vergütung wird das Präsidium – sofern sich diese innerhalb des festgelegten Höchstbetrags von bis zu 60 € bewegt – den Vorschlägen der Fakultäten folgen, ohne dass es hierfür im Antrag einer besonderen Begründung bedarf.

In der wissenschaftlichen Weiterbildung ist eine abweichende Vergütung möglich, wenn die Voraussetzungen des § 34 Abs. 3, insbesondere Satz 3 NHG eingehalten sind und die Weiterbildung nach Trennungsrechnungssätzen kalkuliert ist.

Angaben über die Vergütung von Lehraufträgen gegenüber den vorgesehenen Lehrpersonen dürfen deshalb erst dann gemacht werden, wenn sicher ist, dass die hierfür erforderlichen Haushaltsmittel zur Verfügung stehen und Bedenken gegen die Höhe der vorgesehenen Vergütung nicht bestehen.

Der Studentische Rat der Leibniz Universität Hannover hat in seiner Sitzung am 30.10.2019 gemäß § 20 NHG die nachfolgende Wahlordnung der Studierendenschaft beschlossen. Das Präsidium hat die Wahlordnung am 20.11.2019 genehmigt. Sie tritt am Tage nach ihrer hochschulöffentlichen Bekanntmachung im Verkündungsblatt der Leibniz Universität Hannover in Kraft.

Wahlordnung der Studierendenschaft der Leibniz Universität Hannover

Inhaltsübersicht:

Abschnitt 1: Grundsätze

- § 1 Zusammensetzung
- § 2 Wahl
- § 3 Wahlberechtigung

Abschnitt 2: Wahlvorbereitung

- § 4 Bildung des Studentischen Wahlausschusses
- § 5 Aufgaben des Studentischen Wahlausschusses
- § 6 Vorsitz des Studentischen Wahlausschusses
- § 7 Beschlussfassung
- § 8 Unvereinbarkeit
- § 9 Verschwiegenheitsverpflichtung
- § 10 Wahlausschreibung
- § 11 Inhalt der Wahlausschreibung
- § 12 Einreichung des Wahlvorschlags
- § 13 Inhalt des Wahlvorschlags
- § 14 Inhalt eines Listenvorschlags
- § 15 Zählgemeinschaft
- § 16 Überprüfung der Wahlvorschläge
- § 17 Wahlbekanntmachung
- § 18 Auslegung des WählerInnenverzeichnisses
- § 19 Fortschreibung des WählerInnenverzeichnisses

Abschnitt 3: Wahldurchführung

- § 20 Wahltermin
- § 21 Wahlunterlagen
- § 22 Wahlauf Ruf
- § 23 Wahlvorgang
- § 24 Authentifizierung
- § 25 Stimmabgabe
- § 26 Pflichten des Wahlausschusses

Abschnitt 4: Ergebnisfeststellung

- § 27 Auszählung
- § 28 Ergebnisfeststellung
- § 29 Ergebnisfeststellung bei Zählgemeinschaften
- § 30 Veröffentlichung des Ergebnisses
- § 31 Störungen bei der elektronischen Wahl
- § 32 Technische Anforderungen

Abschnitt 5: Wahlprüfung

§ 33 Benachrichtigung der gewählten Vertreterinnen

§ 34 Wahleinsprüche

Abschnitt 6: Sonstiges

§ 35 Geltung der Wahlordnung der Leibniz Universität Hannover

§ 36 Inkrafttreten

Abschnitt 1: Grundsätze

§ 1 Zusammensetzung

- (1) Fachschaftsräte umfassen ein Mitglied je angefangene 100 Studierende der Fachschaft, mindestens jedoch vier Mitglieder.
- (2) Der Studentische Rat besteht aus direkt gewählten und von den Fachschaftsräten delegierten VertreterInnen. Näheres regelt die Satzung.

§ 2 Wahl

- (1) Die Mitglieder der Fachschaftsräte und die direkt gewählten Mitglieder des Studentischen Rates werden durch allgemeine, freie, gleiche, geheime und direkte internetbasierte Online-Wahl (elektronische Wahl) gewählt.
- (2) Die Wahl erfolgt nach dem Prinzip der mit der Personenwahl verbundenen Listenwahl. EinzelkandidatInnen sind zugelassen. Die Auszählung erfolgt nach dem Sainte-Laguë-Verfahren.
- (3) Es wird nach den Grundsätzen der Mehrheitswahl gewählt, wenn:
 - nur Einzelwahlvorschläge vorliegen oder
 - nur ein Listenwahlvorschlag vorliegt.
- (4) Die Amtszeit beträgt in der Regel 2 Semester.

§ 3 Wahlberechtigung

Wahlberechtigt sind alle immatrikulierten Studierenden der Leibniz Universität Hannover.

Abschnitt 2: Wahlvorbereitung

§ 4 Bildung des Studentischen Wahlausschusses

- (1) Der studentische Wahlausschuss (SWA) besteht aus fünf Studierenden der Leibniz Universität Hannover und ihren fünf StellvertreterInnen. Die Gruppen im StuRa mit den meisten Stimmen benennen je ein Mitglied und eineN StellvertreterIn des studentischen Wahlausschusses. EinzelkandidatInnen zählen hierbei wie Gruppen; bei Stimmgleichheit entscheidet das Los. Die Reihenfolge der Benennung folgt der Größe der Gruppe. Sind weniger als fünf Gruppen im StuRa vorhanden, so wird das Verfahren nach Satz 2 und 3 so oft wiederholt, bis alle fünf Sitze besetzt sind. Kommt die Benennung nicht zustande, setzt das Präsidium der Universität einen SWA ein.
- (2) Die Amtszeit des SWA endet mit dem Zusammentritt eines neu gewählten SWA für die nächsten turnusmäßigen Wahlen.

§ 5 Aufgaben des Studentischen Wahlausschusses

- (1) Der SWA überwacht die Ordnungsmäßigkeit der Wahl nach dieser Wahlordnung und ist für diese Wahlen verantwortlich.
- (2) Der SWA entscheidet Zweifelsfragen bei der Wahlhandlung und Stimmauszählung und stellt das Wahlergebnis fest. Der SWA prüft die Gültigkeit der Wahl und beschließt über Beschwerden wegen zurückgewiesener Wahlvorschläge.
- (3) Er stellt die Anzahl der Mitglieder der einzelnen Fachschaftsräte auf Grund der Studierendenstatistik des vorangegangenen Semesters fest.

§ 6 Vorsitz des Studentischen Wahlausschusses

Der/die WahlleiterIn lädt zur ersten Sitzung des SWA ein, er/sie oder einE BeauftragteR leitet diese Sitzung, bis sich der SWA eineN VorsitzendeN und eineN StellvertretendeN aus seiner Mitte gewählt hat. Zu den folgenden Sitzungen lädt der/die Vorsitzende ein. Unterbleibt die Einladung, so lädt der/die WahlleiterIn ein.

§ 7 Beschlussfassung

- (1) Der SWA ist bei ordnungsgemäßer Ladung aller Mitglieder beschlussfähig, wenn mindestens drei Mitglieder anwesend sind. Es ist ordnungsgemäß geladen worden, wenn die Einladungsschreiben drei Tage vor der Sitzung abgesandt wurden oder auf einer Sitzung Einverständnis über einen neuen Termin erzielt wurde. In diesem Fall sind Abwesende sofort über den neuen Termin zu unterrichten.
- (2) Beschlüsse werden mit der Mehrheit der abgegebenen Stimmen der anwesenden Mitglieder gefasst. Bei Beschlussunfähigkeit entscheidet in dringenden Fällen der/die WahlleiterIn.

§ 8 Unvereinbarkeit

Die Mitglieder des SWA dürfen nicht zugleich WahlkandidatInnen sein.

§ 9 Verschwiegenheitsverpflichtung

Die Mitglieder des SWA und ihre Stellvertreter sind zur verantwortungsbewussten Ausübung ihres Amtes und zur Verschwiegenheit verpflichtet, d. h. sie dürfen keine vertraulichen Daten an unberechtigte Außenstehende weitergeben.

§ 10 Wahlausschreibung

Der/die WahlleiterIn schreibt die Wahlen zu den Fachschaftsräten und für die direkt gewählten Mitglieder des Studentischen Rates in Abstimmung mit den Gremienwahlen der Universität aus. Die Wahlausschreibung wird an den Anschlagstellen im Lichthof des Hauptgebäudes, der Fakultäten und der zentralen Einrichtungen in auffälliger Weise ausgehängt.

§ 11 Inhalt der Wahlausschreibung

Die Wahlausschreibung enthält mindestens:

- a.) die Anzahl der in den einzelnen Fachschaften zu wählenden Mitglieder der Fachschaftsräte,
- b.) die Anzahl der direkt zu wählenden Mitglieder des Studentischen Rates,
- c.) die Aufforderung, Wahlvorschläge an den/die WahlleiterIn einzureichen,
- d.) die Bedingungen, die ein Wahlvorschlag erfüllen muss,
- e.) den Zeitpunkt, bis zu dem Wahlvorschläge entgegen genommen werden,
- f.) die Aufforderung zur Einsichtnahme in das WählerInnenverzeichnis mit einem Hinweis auf die Möglichkeit, Einspruch einzulegen sowie auf Ort und Zeit für die Abgabe von Einsprüchen.

§ 12 Einreichung des Wahlvorschlags

- (1) Die Kandidatur zu den studentischen Gremien erfolgt durch Einreichung eines Wahlvorschlages bis zum Ablauf der durch den Wahlausschuss beschlossenen und in der Wahlausschreibung veröffentlichten Frist. Diese beträgt mindestens 14 Tage und endet spätestens drei Wochen vor dem ersten Wahltag.
- (2) Eine Verlängerung der Frist kann vom SWA beschlossen werden. Die Frist ist für die einzelnen studentischen Gremien zu verlängern, wenn weniger Wahlvorschläge eingereicht wurden als in diesem Gremium Sitze zu vergeben sind.
- (3) Sollten auch nach Verlängerung der Einreichungsfrist weniger oder gleich viele KandidatInnen wie Sitze in einem Gremium vorhanden sein, so gelten die eingereichten Wahlvorschläge automatisch als gewählt. Eine Wahl entfällt.

§ 13 Inhalt des Wahlvorschlags

JedeR KandidatIn reicht einen Wahlvorschlag ein. Bei Listenvorschlägen können mehrere Wahlvorschläge auf einer Vorschlagsliste zusammengefasst werden. Jeder Wahlvorschlag muss enthalten:

- a.) Namen, Vorname, Fachrichtung, Matrikelnummer, die genaue Anschrift, E-Mail-Adresse, sowie, wenn möglich, Telefonnummer der/des KandidatIn/en,
- b.) die Erklärung der/des KandidatIn/en, dass er/sie bereit ist, ein Amt in der studentischen Selbstverwaltung zu übernehmen,
- c.) den Namen der Liste bei Listenkandidatur.

§ 14 Inhalt eines Listenvorschlags

Mindestens zwei KandidatInnen können sich zu einer Liste zusammenschließen. Die KandidatInnen müssen zusätzlich zu den Bestimmungen in § 12 einen Listenwahlvorschlag einreichen, der die Namen der KandidatInnen in der von ihnen selbst festgelegten Reihenfolge enthält. Ein Protokoll über die demokratisch festgelegte Anordnung der Namen ist dem/der WahlleiterIn einzureichen.

§ 15 Zählgemeinschaft

Mindestens zwei Listen können sich zu einer Zählgemeinschaft zusammenschließen. Der Wahlvorschlag enthält den Namen der Zählgemeinschaft zusätzlich zu dem der Listenverbindung. Die §§ 13 und 14 gelten entsprechend.

§ 16 Überprüfung der Wahlvorschläge

- (1) Der SWA lässt die Wahlvorschläge nach Überprüfung ihrer Vollständigkeit zur Wahl zu. Bei Unvollständigkeit ist die/der betroffene KandidatIn zu benachrichtigen. Erfolgt binnen drei Tagen nach Benachrichtigung keine Berichtigung, so wird die/der KandidatIn gestrichen. Die Streichung wird ihr/ihm mitgeteilt.
- (2) Verspätet eingegangene Wahlvorschläge bleiben unberücksichtigt.
- (3) Gegen Streichung oder Zurückweisung kann innerhalb von drei Tagen beim Ältestenrat Beschwerde eingelegt werden. Der Ältestenrat hat binnen drei Werktagen zu entscheiden.

§ 17 Wahlbekanntmachung

Der/die WahlleiterIn veröffentlicht in der Wahlbekanntmachung alle zugelassen Wahlvorschläge, die unverzüglich und bis zur Beendigung der Wahl an den Anschlagbrettern im Lichthof des Hauptgebäudes, der Fakultäten und in zentralen Einrichtungen durch Aushang bekanntzumachen sind. Der Aushang soll binnen zehn Werktagen nach dem Abgabetermin für die Wahlvorschläge erfolgt sein und soll gemeinsam mit der Wahlbekanntmachung für die Gremienwahlen der Universität erfolgen. Der Aushang muss die zugelassenen Wahlvorschläge mit Vor- und Zunamen beinhalten. Ferner enthält er:

- a.) die Aufforderung zur Stimmabgabe,
- b.) die Bestimmungen, die jedeR WählerIn zwecks Durchführung einer ordnungsgemäßen Wahl zu beachten hat,
- c.) Ort und Zeit der Wahl,
- d.) Ort und Zeit der öffentlichen Stimmenauszählung.

§ 18 Auslegung des WählerInnenverzeichnisses

Wählen und gewählt werden darf nur, wer zum Zeitpunkt der Wahl immatrikuliert und demzufolge ins WählerInnenverzeichnis eingetragen ist. Dabei richtet sich die Wahlberechtigung nach dem ersten gewählten Studienfach, auf Antrag stattdessen nach dem Zweifach. Der/die WahlleiterIn hat zu Beginn der Vorlesungszeit des Wintersemesters alle zu dieser Wahl wahlberechtigten Studierenden in ein WählerInnenverzeichnis eintragen zu lassen. Das WählerInnenverzeichnis ist in Ausfertigungen oder Auszügen im Wahlamt der Universität zur Einsichtnahme auszulegen. Der Auslegungszeitraum umfasst die Einreichungsfrist für die Wahlvorschläge. Das WählerInnenverzeichnis wird sofort nach Ende der Auslegung vom SWA nach Behandlung aller Einsprüche durch Beschluss festgestellt.

§ 19 Fortschreibung des WählerInnenverzeichnisses

- (1) Für die Ausübung des aktiven Wahlrechts ist das festgestellte WählerInnenverzeichnis von Amts wegen oder auf Grund von Anträgen, die bis zu einem in der Wahlbekanntmachung festgesetzten Zeitpunkt eingehen, durch nachträgliche Eintragungen fortzuschreiben. Die Frist für nachträgliche Eintragungen darf frühestens mit dem siebten Tage vor Beginn des Wahlzeitraums enden. Wer nach Ablauf dieser Frist Mitglied der Studierendenschaft wird, ist nicht wahlberechtigt.
- (2) Über die nachträgliche Eintragung entscheidet der/die WahlleiterIn. Er hat den SWA darüber zu unterrichten. Dieser kann die Entscheidung des/der WahlleiterIn aufheben und durch eine eigene Entscheidung ersetzen.
- (3) Über die nachträgliche Eintragung werden die betroffenen Wahlberechtigten durch die Wahlleitung benachrichtigt.

- (4) Das WählerInnenverzeichnis kann von dem/der WahlleiterIn jederzeit berichtigt werden, wenn es unwesentliche Fehler, Unstimmigkeiten oder Schreibversehen enthält. Die Berichtigung ist als solche kenntlich zu machen und mit Datum und Unterschrift des/der WahlleiterIn oder einer/eines Beauftragten zu versehen.

Abschnitt 3: Wahldurchführung

§ 20 Wahltermin

Es wird in der Regel gleichzeitig und in organisatorischer Einheit mit den Gremienwahlen der Universität gewählt. Eine abweichende Regelung der Wahlzeit muss der/die WahlleiterIn gegenüber dem SWA begründen.

§ 21 Wahlunterlagen

Der/die WahlleiterIn versendet die Wahlunterlagen in der Regel elektronisch an die Wahlberechtigten. Die Wahlunterlagen bestehen aus der Benachrichtigung über die Wahl mit Angabe des Wahlzeitraums sowie Informationsmaterial. Über die Eintragung in das Wählerverzeichnis erhält der oder die Wahlberechtigte in der Regel spätestens zwei Wochen vor der Wahl eine elektronische oder schriftliche Benachrichtigung. Das Informationsmaterial enthält insbesondere Erläuterungen zum Wahlzugang und zur Durchführung der Wahl sowie zur Nutzung des Portals zur Online-Stimmabgabe. Der/die WahlleiterIn kann weitergehende Informationen beifügen.

§ 22 Wahlaufruf

Der AStA soll spätestens eine Woche vor der Wahl auf Ort und Zeit der Wahl durch Plakate, Rundschreiben an Institute und Wohnheime sowie durch Handzettel hinweisen.

§ 23 Wahlvorgang

- (1) Die Freigabe und das Schließen des Wahlvorgangs werden von der Wahlleitung festgelegt.
- (2) Die elektronische Wahl ist während der regulären Öffnungszeiten an den bekannt gemachten Standorten oder jederzeit über einen Computer möglich, der über das Internet mit dem Portal zur Online-Stimmabgabe verbunden ist.
- (3) Der Stimmzettel enthält die Listen und die EinzelkandidatInnen in der Reihenfolge ihrer bei den letzten Wahlen errungenen Stimmenzahl sowie die Namen der Zählgemeinschaften.
- (4) Bei Gleichheit der Stimmenzahl entscheidet die Reihenfolge des Eingangs der Wahlvorschläge. Bei gleichzeitigem Eingang entscheidet das Los.
- (5) Bei erstmalig kandidierenden Listen bzw. Einzelkandidatinnen entscheidet die Reihenfolge des Eingangs der Wahlvorschläge. Bei gleichzeitigem Eingang entscheidet das Los.
- (6) Die Reihenfolge der KandidatInnen innerhalb einer Liste bestimmt sich nach § 14. Die KandidatInnenfolge auf den Listen wird durchnummeriert.
- (7) Auf dem Stimmzettel ist deutlich darauf hinzuweisen, wie viele KandidatInnen höchstens anzukreuzen sind. Bei Listenwahl ist zusätzlich darauf hinzuweisen, dass die Stimme für einen KandidatIn auch zugunsten der gesamten Liste gezählt wird.

§ 24 Authentifizierung

- (1) Die Stimmabgabe erfordert eine vorherige Authentifizierung.
- (2) Findet die Authentifizierung über das hochschuleigene Authentifizierungssystem (zentrales Identitätsmanagement) statt, erfolgt sie mit den in diesem System vergebenen Zugangsdaten.
- (3) Der Zugang zum Portal zur Online-Stimmabgabe ist während des Wahlzeitraums bis zur endgültigen Abgabe der Stimme mehrfach möglich.
- (4) Vor der Stimmabgabe ist die wahlberechtigte Person darauf hinzuweisen, dass die Stimmabgabe geheim und frei zu erfolgen hat.
- (5) Nach Stimmabgabe ist eine erneute Authentifizierung zu Wahlzwecken nicht mehr zulässig.
- (6) Auf die Daten, die durch die Authentifizierung zu Zwecken der Durchführung der Wahl erzeugt werden, darf zu anderen Zwecken als zur Durchführung der Wahl nicht zugegriffen werden.

§ 25 Stimmabgabe

- (1) Die Stimmabgabe erfolgt in elektronischer Form durch Ausfüllen des elektronischen Stimmzettels. Der elektronische Stimmzettel muss alle Wahlvorschläge enthalten. Jede Wählerin und jeder Wähler hat nur eine Stimme. Bei Mehrheitswahlen in einem Wahlbereich können so viele BewerberInnen gewählt werden, wie Sitze auf die Gruppe entfallen. Stimmenhäufung auf eine Bewerberin oder einen Bewerber ist unwirksam.
- (2) Das Ausfüllen des elektronischen Stimmzettels erfolgt durch Markierung. Die wahlberechtigte Person besitzt bis zur endgültigen Stimmabgabe das Recht, ihre Eingabe zu korrigieren oder die Wahl abzubrechen. Kommt es nicht zu einer endgültigen Stimmabgabe, werden die Markierungen nicht fixiert. Die Abgabe von weniger Stimmen als rechtlich gestattet und die Abgabe eines leeren Stimmzettels ist zulässig, ebenso wie eine ungültige Stimmabgabe.
- (3) Die Abgabe des elektronischen Stimmzettels führt noch nicht zur endgültigen Stimmabgabe. Vielmehr sind der wahlberechtigten Person nach Abgabe des elektronischen Stimmzettels die ausgefüllten Wahlvorschläge zur Bestätigung anzuzeigen. Die Ablehnung dieser Endfassung führt zum elektronischen Stimmzettel zurück, bei dem die Markierungen noch bestehen. Die Bestätigung des abgegebenen elektronischen Stimmzettels führt zur endgültigen Stimmabgabe. An die Bestätigung schließt sich die Übermittlung der endgültigen Stimmabgabe an. Die Übermittlung muss für die wahlberechtigte Person am Bildschirm erkennbar sein. Mit dem Hinweis auf die erfolgreiche endgültige Stimmabgabe gilt diese als vollzogen. Eine erneute Stimmabgabe ist unzulässig.
- (4) Ein Ausdruck des elektronischen Stimmzettels, der Markierungen der abgegebenen Stimme oder der endgültigen Stimmabgabe und vergleichbare Verstärkungen sind nicht zulässig. Die einzelnen Schritte des Wahlvorganges dürfen nicht gleichzeitig angezeigt werden.
- (5) Die Stimmabgabe ist völlig getrennt von der Authentifizierung abzugeben. Eine Verknüpfung zwischen der Identität des Wahlberechtigten und der Stimmabgabe darf in keiner Weise hergestellt werden.
- (6) Inaktivität gilt in jeder Phase der elektronischen Stimmabgabe als Abmeldung.

§ 26 Pflichten des Wahlausschusses

Ein VertreterIn des SWA muss während der Wahlzeiten ständig zur Entgegennahme von Beschwerden erreichbar sein. JedeR Studierende hat das Recht, sich über die Durchführung der Wahl beim SWA zu beschweren. Die/der VertreterIn des SWA muss Beschwerden sofort nachgehen.

Abschnitt 4: Ergebnisfeststellung

§ 27 Auszählung

- (1) Nach Beendigung der Online-Wahl wird die Urne elektronisch durch das System ausgezählt. Die Öffnung des elektronisch bereitgestellten Ergebnisses erfolgt hochschulöffentlich in Anwesenheit der Wahlleitung. Die Wahlleitung veranlasst unverzüglich nach Bereitstellung des Abstimmungsergebnisses die Auswertung der abgegebenen Stimmen inklusive der Sitzverteilung.
- (2) Die auf jeden Wahlvorschlag entfallenden gültigen Stimmen werden zusammengezählt. Ungültig sind Stimmen, wenn der Stimmzettel
 1. keinen Stimmabgabevermerk enthält,
 2. mehr als die jeweils zulässigen Stimmabgabevermerke enthält,
 3. als ungültig gekennzeichnet ist, sofern diese Option bereitgestellt wird.
- (3) Alle Datensätze der elektronischen Internetwahl sind in geeigneter Weise zu speichern. Über die Auszählung ist eine Niederschrift anzufertigen (§ 5 Abs. 4).
- (4) Der/die WahlleiterIn gewährt auf Antrag bei berechtigtem Interesse die Möglichkeit, anhand der von der elektronischen Wahlurne erzeugten Datei die Ordnungsmäßigkeit der Auszählung zu prüfen. Die Frist für die Stellung der Anträge bestimmt der/die WahlleiterIn.

§ 28 Ergebnisfeststellung

- (1) Die für eineN ListenkandidatIn abgegebene Stimme zählt einerseits für die Liste insgesamt und bestimmt andererseits den Platz der/des KandidatIn auf der Liste.

- (2) Bis zu der nach § 1 bestimmten vollständigen Zahl der Mitglieder jedes Fachschaftsrates wird nach Sainte-Laguë die Anzahl der gewählten KandidatInnen einer Liste und der EinzelkandidatInnen festgestellt.
- (3) Die der Liste zustehenden Sitze werden von den KandidatInnen mit den höchsten Stimmzahlen besetzt.
- (4) Freiwerdende Sitze von ListenkandidatInnen werden durch die nach der Stimmzahl folgenden KandidatInnen ihrer Liste besetzt. Fehlt eine Nachfolge in der gleichen Liste oder wird der Sitz einer/ eines EinzelkandidatIn frei, so wird der Sitz durch die/den KandidatIn besetzt, die/der oder dessen Liste nach dem Sainte-Laguë-Verfahren den nächsten Sitz besetzen würde.
- (5) Gewählte ListenkandidatInnen werden im Falle ihrer Verhinderung von nicht gewählten KandidatInnen vertreten. Dies müssen nicht die KandidatInnen sein, die im Falle des vorzeitigen Ausscheidens von Mitgliedern als Ersatzpersonen nachrücken würden.
- (6) Gleiches gilt für die direkt zu wählenden Mitglieder des Studentischen Rates. Die Anzahl der Mitglieder des Studentischen Rates ergibt sich nach § 9.1 der studentischen Satzung.

§ 29 Ergebnisfeststellung bei Zählgemeinschaften

Bei Zählgemeinschaften nach §15 erfolgt die Ergebnisfeststellung entsprechend § 30, indem zunächst die auf die Zählgemeinschaft entfallenden Sitze ermittelt werden.

§ 30 Veröffentlichung des Ergebnisses

Das Wahlergebnis ist an den in § 17 angegebenen Orten vollständig zu veröffentlichen.

§ 31 Störungen bei der elektronischen Wahl

- (1) Ist die elektronische Stimmabgabe während der Wahlfrist aus Gründen, die die Universität zu vertreten hat, nicht möglich, kann der/die WahlleiterIn die Wahlfrist verlängern. Die Verlängerung muss allgemein bekannt gegeben werden.
- (2) Werden während der elektronischen Wahl Störungen bekannt, die ohne Gefahr eines vorzeitigen Bekanntwerdens oder Löschens der bereits abgegebenen Stimmen behoben werden können und ist zugleich eine mögliche Stimmenmanipulation ausgeschlossen, kann die Wahlleitung solche Störungen beheben oder beheben lassen und die Wahl fortsetzen.
- (3) Ist eine Manipulation nicht ausgeschlossen, ist die Wahl abubrechen.
- (4) Bei sonstigen Störungen entscheidet die Wahlleitung nach sachgemäßem Ermessen, wie auf die Störung zu reagieren ist. Maßgeblich ist dabei das Ausmaß der Beeinträchtigung der relevanten Wahlgrundsätze.

§ 32 Technische Anforderungen

- (1) Elektronische Wahlen dürfen nur dann durchgeführt werden, wenn das verwendete elektronische Wahlsystem aktuellen technischen Standards, insbesondere den Sicherheitsanforderungen für Online-Wahlprodukte des Bundesamtes für Sicherheit in der Informationstechnik, entspricht. Das System muss die in den nachfolgenden Absätzen aufgeführten technischen Spezifikationen besitzen. Die Erfüllung der technischen Anforderungen ist durch geeignete Unterlagen nachzuweisen.
- (2) Zur Wahrung des Wahlgeheimnisses müssen elektronische Wahlurne und elektronisches Wahlverzeichnis auf verschiedener Serverhardware geführt werden. Das Wählerverzeichnis soll auf einem universitätseigenen Server gespeichert sein.
- (3) Die Wahlserver müssen vor Angriffen aus dem Netz geschützt sein, insbesondere dürfen nur autorisierte Zugriffe zugelassen werden. Autorisierte Zugriffe sind insbesondere die Überprüfung der Stimmberechtigung, die Speicherung der Stimmabgabe zugelassener Wählerinnen und Wähler, die Registrierung der Stimmabgabe und die Überprüfung auf mehrfacher Ausübung des Stimmrechtes (Wahlzeiten). Es ist durch geeignete technische Maßnahmen zu gewährleisten, dass im Falle des Ausfalles oder der Störung eines Servers oder eines Serverbereiches keine Stimmen unwiederbringlich verloren gehen können.
- (4) Die Datenübermittlung muss verschlüsselt erfolgen, um eine unbemerkte Veränderung der Wahlzeiten zu verhindern. Bei der Übertragung und Verarbeitung der Wahlzeiten ist zu

gewährleisten, dass bei der Registrierung der Stimmabgabe im Wählerverzeichnis kein Zugriff auf den Inhalt der Stimmabgabe möglich ist.

- (5) Die Wählerinnen und Wähler sind über geeignete Sicherungsmaßnahmen zu informieren, mit denen der für die Wahlhandlung genutzte Computer gegen Eingriffe Dritter nach dem aktuellen Stand der Technik geschützt wird. Die Kenntnisnahme der Sicherheitshinweise ist vor der Stimmabgabe durch den Wähler verbindlich in elektronischer Form zu bestätigen. Auf die Möglichkeit der Nutzung gesicherter Geräte innerhalb der Universität gem. § 23 Abs. 2 1. Alternative kann verwiesen werden.

Abschnitt 5: Wahlprüfung

§ 33 Benachrichtigung der gewählten Vertreterinnen

Der SWA benachrichtigt die gewählten Mitglieder über ihre Wahl und Amtszeit; dasselbe gilt beim Ausscheiden von Mitgliedern gegenüber den nachrückenden Mitgliedern.

§ 34 Wahleinsprüche

- (1) Verstoßen die Wahlen gegen die Satzung oder gegen diese Wahlordnung und ist durch diesen Verstoß das Ergebnis der Wahlen verfälscht worden, so sind die Wahlen für ungültig zu erklären.
- (2) JedeR Wahlberechtigte kann die Wahl innerhalb einer Woche nach Bekanntgabe des Wahlergebnisses beim SWA durch begründeten Einspruch anfechten. Der SWA entscheidet über den Einspruch binnen einer Woche.
- (3) Wird die Wahl zu einem Fachschaftratsrat für ungültig erklärt, so sind hierfür Neuwahlen auszuschreiben. Die Fristen der Satzung und dieser Wahlordnung sind für die Neuwahl anzuwenden.

Abschnitt 6: Sonstiges

§ 35 Geltung der Wahlordnung der Leibniz Universität Hannover

Soweit in dieser Wahlordnung keine abweichende Bestimmung getroffen wurde, gelten die Vorschriften der Wahlordnung der Leibniz Universität Hannover in der jeweils gültigen Fassung entsprechend.

§ 36 Inkrafttreten

Diese Wahlordnung tritt mit der Genehmigung des Präsidiums der Leibniz Universität Hannover am Tage nach ihrer hochschulöffentlichen Bekanntmachung in Kraft. Gleichzeitig tritt die bisherige Wahlordnung außer Kraft.

B. Bekanntmachungen nach § 78 Abs. 2 NPersVG

Die nachfolgende Dienstvereinbarung, unterzeichnet vom Präsidium der Gottfried Wilhelm Leibniz Universität Hannover am 04.10.2019 sowie vom Personalrat der Gottfried Wilhelm Leibniz Universität Hannover am 11.09.2019, ist abgeschlossen worden. Sie trat zum 01.10.2019 in Kraft.

Dienstvereinbarung gemäß § 78 NPersVG über die Einführung einer Inventarisierungssoftware (Inventory Tool) an der Gottfried Wilhelm Leibniz Universität Hannover

zwischen

**der Leibniz Universität Hannover, vertreten durch das Präsidium, dieses vertreten durch den
Präsidenten**

und

dem Personalrat der Leibniz Universität Hannover

Präambel

Für einen ordnungsgemäßen und sicheren IT-Betrieb ist es notwendig, die im Einsatz befindlichen IT-Systeme und die darauf eingesetzte Software zu kennen, z.B. für:

- Konformität bzgl. der Software-Lizenzen und -Verträge
- Feststellen auslaufender Wartung für zentrale IT-Komponenten
- reibungsloses Software-Upgrade ohne ungeplante Verfügbarkeitseinschränkung aufgrund unzureichender Hardware-Ausstattung
- planmäßige Außerbetriebnahme ungenutzter IT
- Auffinden gestörter IT-Komponenten
- Feststellen veralteter oder schadhafter Software-Installationen.

Ein entsprechendes Verzeichnis für alle an der Leibniz Universität Hannover im Einsatz befindlichen Geräte ohne technische Unterstützung zu erstellen, ist mit vertretbarem Aufwand nicht möglich. Daher wird an der Leibniz Universität Hannover eine Inventarisierung für dienstliche Client- und Server-Systeme eingeführt, bei der die Hard- und Software-Ausstattung automatisiert und regelmäßig erhoben und an einen zentralen Server übermittelt wird. Wird ein so inventarisiertes Gerät von nur einer Person genutzt, ist ein eindeutiger Personenbezug möglich. Daher muss der Umgang mit den Daten geregelt werden und die Betroffenen sind über die erhobenen und verarbeiteten Daten zu informieren.

§ 1 Geltungsbereich

Diese Vereinbarung gilt für alle Beschäftigten der Leibniz Universität Hannover und betrifft alle dienstlichen Client- und Server-Systeme.

§ 2 Allgemeine Grundsätze und Definitionen

- (1) Die Inventarisierung dient der Erfassung von IT-Systemen und eingesetzter Software. Sie dient nicht der Erfassung von Nutzenden, Nutzungsdauern oder Bezügen zwischen Nutzenden und Anwendungen.
- (2) Betroffene sind über Rundschreiben mit Verweis auf diese Dienstvereinbarung darüber zu informieren, welche Daten erhoben und verarbeitet werden.
- (3) Die übermittelten Datensätze können von Nutzenden des jeweiligen Gerätes über eine lokale Textdatei eingesehen werden.

§ 3 Erhobene Daten

- (1) Auf den betroffenen Systemen werden folgende Daten automatisch für die Inventarisierung erhoben:
 - Informationen über die Hardware-Ausstattung (festverbaute Komponenten sowie angesteckte, eingeschaltete Peripherie)
 - Version und ggf. Lizenzaktivierung/-art des genutzten Betriebssystems
 - Informationen über die installierte Software (Anwendungen und Updates; für Windows vergleichbar der Programme-Liste in der Systemsteuerung)
 - Computernamen und IP-Adresse, Domänenzugehörigkeit
 - Zeitpunkt der (jüngsten) Inventarisierung.
- (2) Die vom Tool erhobenen Daten liegen nach einem Inventarisierungs-Durchlauf in einer Datei auf dem Gerät. Diese Datei lässt sich durch die Systemadministratoren und Nutzende des Systems ansehen. Der individuelle Pfad dieser Datei variiert je nach Betriebssystem, Betriebssystemversion und Sprache. Er wird auf den Webseiten des LUIS dokumentiert und kann bei Bedarf auch über den LUIS-Helpdesk erfragt werden.
- (3) Die Daten werden täglich während der Betriebszeit des Systems erhoben. Die Erhebung erfolgt im Hintergrund und führt auf üblicher Hardware zu keiner merklichen Nutzungseinschränkung.
- (4) Zu einem Rechner kann zusätzlich die Organisationseinheit hinterlegt werden, der das System zugeordnet ist. Diese kann nicht automatisch erhoben, sondern nur durch eine administrierende Person der Einrichtung initial manuell eingetragen werden. Die Speicherung erfolgt auf dem zentralen Inventarisierungsserver. Änderungen können auf Anfrage durch administratives Personal des zentralen Inventarisierungsservers vorgenommen werden.

§ 4 Zweck der Datenerhebung

- (1) Die erhobenen Daten dienen dem Betrieb der IT und der Planung der IT-Landschaft im Rahmen der IT-Administration. Dieses bedeutet im Einzelnen:
 - Grundlagenermittlung für ein Ausrollen von Software
 - Zielgerichteter Support von Anwenderinnen, Anwendern, Administratorinnen und Administratoren bei Rechner-Problemen
 - Grundlagenermittlung für die Lizenzverwaltung (Ist-Stand der eingesetzten Softwareprodukte)
 - Planung des Hard- & Software- und des Service-Bedarfs
 - Übersicht über die IT-Systeme.
- (2) Darüber hinaus sind die Daten grundlegend für die IT-Sicherheit (von der Konzeption über die Auswahl der Maßnahmen und Erkennung von Problemen bis hin zur Reaktion auf Sicherheitsvorfälle):
 - Übersicht über die IT-Landschaft der LUH
 - Zuordnen von IT-Geräten zu Organisationseinheiten der LUH (Zuständigkeit)
 - Finden veralteter (und damit häufig anfälliger) oder sogar bösartiger Programme
 - Erkennen ungewarteter IT-Systeme.

§ 5 Zugriffsrechte

- (1) Die Erhebung und Nutzung der in § 3 genannten Daten ist zum Zwecke der IT-Administration datenschutzrechtlich zulässig. Die aggregierten erhobenen Daten stehen zunächst zentral im LUIS zur Verfügung. Eine Weitergabe personenbezogener Daten an die jeweiligen Einrichtungen ist zum Zwecke der IT-Administration nur an durch die Einrichtungen belehrte Personen gestattet (siehe Anlage).
- (2) Die von einem System zuletzt erhobenen und übermittelten Daten können aus Transparenzgründen auf dem jeweiligen Gerät von allen Nutzenden (einschließlich der Administratorinnen und Administratoren) dieses Gerätes eingesehen werden.

§ 6 Verhaltens- und Leistungskontrollen

Verhaltens- und Leistungskontrollen durch die bei der Inventarisierung verwendeten technischen Systeme oder die im Rahmen der Inventarisierung erhobenen Daten oder personenbezogene und vergleichende Auswertungen sind untersagt, ein Verstoß kann dienstrechtliche Konsequenzen nach sich ziehen.

§ 7 Inkrafttreten, Geltungsdauer, Kündigung

- (1) Diese Vereinbarung tritt mit Wirkung vom 01.10.2019 in Kraft.
- (2) Diese Vereinbarung kann jederzeit im gegenseitigen Einvernehmen der Vertragspartner geändert werden. Veränderungen oder Ergänzungen bedürfen der Schriftform.

Anlage: Formular Bestätigung durch Programmanwender (Systemadministrator)

Hannover, den 04.10.2019

Hannover, den 11.09.2019

.....
Prof. Dr. iur. Volker Epping
Präsident

.....
Elvira Grube
Vorsitzende des Personalrats

Anlage 1 zur Dienstvereinbarung Inventory-Tool

Bestätigung durch Programmanwender/Programmanwenderin (Administration, IT-Beauftragte)

Bestätigung gemäß Absatz 9.2 der „Vereinbarung über die Ziele und Grundsätze bei der Einführung und Nutzung von Fernsteuerungs-, Fernwartungs- und Auswertungssoftware“ vom April 2007 und gemäß § 5 Absatz 1 der Dienstvereinbarung gemäß § 78 NPersVG über die Einführung einer Inventarisierungssoftware (Inventory Tool) an der Gottfried Wilhelm Leibniz Universität Hannover:

Bestätigung durch Frau / Herrn _____

Organisationseinheit _____

Hiermit bestätige ich, dass ich im folgenden Verfahren geschult worden bin:

- Softwareinventarisierung in meiner Organisationseinheit

Ich wurde dabei über die Funktionalitäten der Programme, die technischen Möglichkeiten und die Einsatzbereiche aufgeklärt. Außerdem wurde mir die „Vereinbarung über die Ziele und Grundsätze bei der Einführung und Nutzung von Fernsteuerungs-, Fernwartungs-, Auswertungssoftware“ in der aktuellen Fassung¹ sowie die „Dienstvereinbarung gemäß § 78 NPersVG über die Einführung einer Inventarisierungssoftware (Inventory Tool) an der Gottfried Wilhelm Leibniz Universität Hannover“² erläutert und ausgehändigt.

Insbesondere wurde ich über die Bedingungen und Risiken der Nutzung der Software aufgeklärt und über das Verbot einer Verhaltens- und Leistungskontrolle der betroffenen Benutzerinnen und Benutzer sowie über meine Sorgfaltspflicht im Umgang mit dem Programm zum Schutz der Datenintegrität in Kenntnis gesetzt.

Mir ist bekannt, dass diese Bestätigung zu meiner Personalakte genommen wird.

Ort, Datum, Unterschrift

¹ vgl. Nds.MBl. 20/2007, S.401ff.

[https://www.niedersachsen.de/download/66293/Nds. MBl. Nr. 20 2007 vom 23.05.2007 S. 401-408.pdf](https://www.niedersachsen.de/download/66293/Nds._MBl._Nr._20_2007_vom_23.05.2007_S._401-408.pdf)

² vgl. Verkündungsblatt 17/2019

Die nachfolgende Dienstvereinbarung, unterzeichnet vom Präsidenten der Gottfried Wilhelm Leibniz Universität Hannover am 16.10.2019 sowie vom Personalrat der Gottfried Wilhelm Leibniz Universität Hannover am 23.10.2019, ist abgeschlossen worden. Sie tritt zum 01.11.2019 in Kraft. Die Anlagen zu dieser Dienstvereinbarung können auf Anfrage bei Herrn Dietrich im Personaldezernat (Sachgebiet 21) eingesehen werden.

**Dienstvereinbarung
über den Betrieb des Forschungsinformationssystems Pure
zwischen der Leibniz Universität Hannover und
dem Personalrat der Leibniz Universität Hannover**

1 Präambel

Die Leibniz Universität Hannover führt die Software Pure der Firma Elsevier als Forschungsinformationssystem (FIS) ein. Das FIS umfasst die Möglichkeit, Publikationen (inkl. Patente), Forschungsdaten, Anträge, Bewilligungen und Projekte sowie Forschungsinfrastruktur (Geräte), Auszeichnungen und Aktivitäten über Metadaten nachzuweisen und Lebensläufe zu führen. Mit diesen Informationen ermöglicht das FIS einen Überblick über das Portfolio der Forschungsleistungen der LUH für die Außendarstellung. Die vorhandenen Möglichkeiten, Informationen zusammenzustellen, unterstützen die Universität außerdem dabei, ihren Berichtspflichten nachzukommen. Darüber hinaus dient das FIS der Erstellung einer Hochschulbibliographie. Daher empfiehlt das Präsidium allen Wissenschaftler*innen die Nutzung des FIS.

Das Forschungsinformationssystem wird durch das Dezernat 4 mit Unterstützung der Technischen Informationsbibliothek (TIB) betreut und von den Leibniz Universität IT Services (LUIS) gehostet. Aufgrund der verarbeiteten Daten steht es in engem Zusammenhang mit dem Personalverwaltungssystem SAP-HR bzw. dem zukünftig in SAP-HCM realisierten elektronischen Personen- und Einrichtungsverzeichnis (EPV), der elektronischen Drittmittelakte SAP-FM sowie dem Schnittstellensystem Data Integration Platform (DIP).

Ziel dieser Vereinbarung ist es, im Rahmen einer angemessenen und sinnvollen Nutzung eines Forschungsinformationssystems den Schutz der personenbezogenen Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten. Die Dienststelle und der Personalrat sind sich ferner darüber einig, dass das FIS nicht für eine Überwachung des Verhaltens und eine Arbeits- und/oder Leistungskontrolle genutzt werden darf, vielmehr ist die Gewährleistung eines gemeinsamen Datenbestands mit transparent geregelten Zugriffsmöglichkeiten und die Vermeidung von Redundanz in der Datenhaltung Ziel des Einsatzes des Forschungsinformationssystems. Auswertungen der im FIS nachgewiesenen Forschungsinformationen erfolgen ausschließlich innerhalb der von dieser Dienstvereinbarung und ihren Anlagen gesetzten Grenzen.

2 Gegenstand

Diese Dienstvereinbarung wird gem. §§ 59, 60, 64, 66 und 67 i.V.m. § 78 NPersVG (Niedersächsisches Personalvertretungsgesetz) geschlossen. Für die Verarbeitung personenbezogener Daten bei der Leibniz Universität gelten die Bestimmungen der EU-Datenschutzgrundverordnung und des Niedersächsischen Datenschutzgesetzes (NDSG) in Verbindung mit den §§ 88 ff. des Niedersächsischen Beamtengesetzes (NBG).

Sie löst die Regelungsabrede zur Implementierung und zum Testbetrieb des Forschungsinformationssystems Pure vom 20.08.2014 ab und definiert die Grundsätze für den Betrieb des Forschungsinformationssystems Pure (nachfolgend Forschungsinformationssystem genannt), das der Verwaltung und Bereitstellung von Forschungsinformationen für eine öffentliche Darstellung, Auswertungen und Berichte auf der Grundlage eines konsolidierten und ständig aktuellen Datenbestands dient.

Diese Dienstvereinbarung definiert ebenfalls Grundsätze für die Interaktion des FIS mit angebotenen Quellsystemen, die über Schnittstellen personenbezogene Daten an das Forschungsinformationssystem übergeben und Zielsysteme, an die Daten vom Forschungsinformationssystem geliefert werden. Im

Rahmen dieser Dienstvereinbarung werden die angeschlossenen Systeme dokumentiert und die Datenweitergabe geregelt.

3 Geltungsbereich

Diese Dienstvereinbarung gilt für alle Beschäftigten der Leibniz Universität Hannover. Alle Mitglieder oder Angehörigen der Hochschule, sowie alle sonstigen, nicht vom Geltungsbereich des NPersVG erfassten Nutzer*innen (z.B. Externe, Gäste, Promotionsstudierende) werden in geeigneter Form über diese Dienstvereinbarung informiert.

4 Systembeschreibung, Leistungsumfang

Das Forschungsinformationssystem Pure ist ein Datenbanksystem, in dem Daten zu wissenschaftlich tätigen Personen, Publikationen (inkl. Patenten), Forschungsdaten, Anträgen, Bewilligungen und Projekten sowie Forschungsausstattung (Equipment/Geräte), Auszeichnungen und forschungsbezogene Aktivitäten (wie Konferenzbesuche und Gremientätigkeiten) erfasst und miteinander verknüpft werden können. Auf der Basis der erfassten Daten kann mithilfe des FIS eine Zuordnung von Forschungsinformationen zu den einzelnen Einrichtungen der Leibniz Universität Hannover erfolgen. Eine detaillierte Auflistung und Beschreibung des Forschungsinformationssystems, seinen Quell- und Zielsystemen sowie die Details zu den vorgenommenen Verarbeitungen ergeben sich aus dem Fachkonzept und den weiteren Anlagen der Dienstvereinbarung.

5 Ziel und Zweckbestimmung des Forschungsinformationssystems

Mit dem Forschungsinformationssystem wird den Forschenden, der Hochschulleitung und den Dekanen der Fakultäten eine Unterstützung bei der Erstellung von Berichten und der Ausgabe von Forschungsinformationen auf Webseiten angeboten. Zudem bietet das an das FIS angeschlossene zentrale Forschungsportal eine weitere attraktive Möglichkeit, Forschungsaktivitäten der Wissenschaftler*innen und der Organisationseinheiten der LUH zu präsentieren.

Wesentliche Vorteile sind:

- keine redundante Datenerhebung
- Zugriff auf einen validierten und für alle Nutzer*innen gleichen Datenbestand
- höhere Effizienz und Datenqualität bei der Erstellung von Berichten
- Transparenz dank Kontrolle über die eigenen Daten durch betroffene Person (Intervenierbarkeit)

Details zur Nutzung des Forschungsinformationssystems und seinen Einsatzzwecken finden sich im Fachkonzept und den weiteren Anlagen zur Dienstvereinbarung, wie dem Berichtskonzept.

6 Schutz der Persönlichkeitsrechte, Datenschutz

Dienststelle und Personalrat verfolgen gleichermaßen das Ziel, bei der Verarbeitung personenbezogener Daten die Persönlichkeitsrechte der Beschäftigten zu schützen. Das erfordert die eindeutige Definition von Daten, Aufgaben und Verantwortlichkeiten. Die Details sind im Fachkonzept, im Rechte- und Rollenkonzept, im Datenschutz- und Löschkonzept und in den weiteren Anlagen dieser Dienstvereinbarung in der jeweils geltenden Version dokumentiert.

Anfallende Daten im Sinne dieser Dienstvereinbarung dürfen nur für die hier vereinbarten Zwecke verarbeitet werden. Die im Forschungsinformationssystem zur Verfügung stehenden personenbezogenen Daten sind im Datenkatalog (Anlage 3) mit ihrer Zweckbestimmung abschließend aufgeführt und dokumentiert. Die Auflistung der Datenfelder ist zum gegenwärtigen Stand abschließend. Auch sofern die personenbezogenen Datenfelder mit neuen Releases der Software erweitert werden, erstreckt sich die Nutzung (z.B. für Berichte) ausschließlich auf die im Datenkatalog festgelegten Felder. Im Falle einer Erweiterung der genutzten personenbezogenen Datenfelder gelten die Regelungen unter 0. Die datenschutzrechtlichen Bestimmungen insbesondere der §§ 88 ff. des NBG und des Art. 5 DSGVO sowie des NDSG werden eingehalten.

Das mit dem Datenschutzbeauftragten abgestimmte Datenschutz- und Löschkonzept inkl. einer Risikobewertung im Sinne von Art. 35 DSGVO ergeben sich aus Anlage 7 sowie der Meldung der Verarbeitungstätigkeit gem. Art. 30 DSGVO in Anlage 11.

Die Datenverarbeitung im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO durch Mitarbeiterinnen und Mitarbeiter der TIB wird durch einen Vertrag zur Datenverarbeitung im Auftrag geregelt.

Die Erbringung von Systemservices zur Wiederherstellung und/oder zur Aufrechterhaltung der Betriebsbereitschaft des Gesamtsystems und/oder zur Lieferung neuer Programmstände auf dem Wege der Fernwartung durch Elsevier ist mit einer Vereinbarung zur Auftragsdatenverarbeitung gem. § 6 NDSG als Anlage zum Hauptvertrag mit Elsevier geregelt. Bei Beauftragung weiterer externer Dienstleister, die die Auftragsdatenverarbeitung im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO einschließt, ist ein Vertrag zur Datenverarbeitung im Auftrag erforderlich.

7 Leistungs- und Verhaltenskontrolle

Die Nutzung des Forschungsinformationssystems zu weiteren Zwecken, insbesondere für Zwecke der Leistungs- und Verhaltenskontrolle oder zu Zwecken einer Ermittlung von Grundlagen für dienstliche Beurteilungen, Disziplinarmaßnahmen oder als Grundlage für die Feststellung des Gesundheitszustandes ist ausgeschlossen. Daten, die aus einer unzulässigen Nutzung stammen, dürfen nicht für arbeitsrechtliche Maßnahmen herangezogen werden. Maßnahmen, die auf Informationen beruhen, die unter Verletzung dieser Dienstvereinbarung gewonnen werden, werden nicht durchgeführt. Wird eine missbräuchliche Nutzung festgestellt, ist die Hochschule verpflichtet, die Ursachen dafür unverzüglich abzustellen und erforderliche Maßnahmen einzuleiten.

Die Universität stellt sicher, dass die Nutzergruppe mit Zugang zum Berichtsmodul (s. Anlage 9, Berichtskonzept) des Forschungsinformationssystems auf die Einhaltung dieser Dienstvereinbarung verpflichtet wird (s. Anlage 8, Rechte- und Rollenkonzept).

8 Rechte- und Rollenkonzept, Zugriffsbestimmungen

Die Zugriffsrechte der Nutzer*innen dienen den im Rahmen dieser Dienstvereinbarung zulässigen Aufgaben im Zusammenhang mit dem Betrieb des Forschungsinformationssystems. Das Rechte- und Rollenkonzept mit den Details zu den Berechtigungen der verschiedenen Nutzergruppen ist in Anlage 8 dargestellt und unterliegt der Mitbestimmung des Personalrats. Ein aktuelles Verzeichnis der Rollen und der den Rollen zugeordneten Personen kann auf Anfrage im Dezernat 4 durch den Personalrat eingesehen werden.

9 Berichte und Auswertungen

Alle Berichte und Auswertungen, die im Sinne dieser Vereinbarung personenbezogene Daten enthalten, sind im Berichtskonzept (Anlage 9) aufgeführt und erläutert. Des Weiteren ist in Anlage 9 das Verfahren beschrieben, mit dem neue, noch nicht erfasste Berichtsdefinitionen, die im laufenden Betrieb des FIS entstehen, in Zusammenarbeit mit dem Datenschutzbeauftragten und dem Personalrat geprüft und ggf. freigegeben und erfasst werden.

Es ist ausdrücklich untersagt, mit dem Forschungsinformationssystem erzeugte personenbezogene Auswertungen, die auf nicht öffentlich bereitgestellten Daten basieren, in Fremdsystemen weiter zu verarbeiten. Dies gilt nicht, soweit eine Datenverarbeitung nach § 17 NHG im Rahmen der Erforderlichkeit zur Aufgabenerfüllung oder nach dem Niedersächsischen Datenschutzgesetz (NDSG)/der Datenschutz-Grundverordnung (DSGVO) zulässig ist.

Die Protokolldaten dienen ausschließlich den Zwecken der Gewährleistung der Systemsicherheit und der Analyse und Korrektur technischer Fehler. Der Zugriff auf die entsprechenden Programmfunktionen und die Löschrufen sind im Rechte- und Rollenkonzept (Anlage 8) sowie dem Datenschutz- und Löschkonzept (Anlage 7) erläutert.

10 Schnittstellen

Schnittstellen im Sinne dieser Dienstvereinbarung sind technische Übergabepunkte und Verfahren, durch die andere Systeme (Quellsysteme) Daten an das hier geregelte System übergeben oder durch die Daten des Forschungsinformationssystems an andere Systeme, Funktionen oder Fremdsysteme übergeben werden (Zielsysteme). Eine Auflistung ist mit Kurzbeschreibung als Anlage 4 (Schnittstellen) beigefügt.

Als operative Quellsysteme für das Forschungsinformationssystem dienen das datenführende System für Personen und Einrichtungen der Leibniz Universität Hannover und das datenführende System für Bewilligungsdaten. Es folgt keine Rückgabe von Daten aus dem FIS an diese Systeme. Datenfehler (z.B. Fehler im Namen) werden über die Leitung des Abschnitts Forschungsinformationen im SG 42 des Dezernats 4 oder deren Vertretung an die verantwortliche Organisationseinheit gemeldet. Details zu den Workflows zu Datenübernahme, -ergänzung und -korrektur finden sich im Fachkonzept (Anlage 1). Die einzuspielenden Daten sind im Datenkatalog (Anlage 3) und in den Schnittstellenbeschreibungen (Anlage 5 und Anlage 6) definiert. Die einzuspielenden Daten aus den o.g. Quellsystemen werden von einer separaten Datenbank bereitgestellt. Diese Datenbank findet nur für den Import von Daten nach Pure Verwendung.

Zielsysteme sind Systeme, die öffentlich freigegebene Daten aus dem FIS veröffentlichen, z.B. das öffentliche Forschungsportal, die TYPO3-Webseiten und ggf. weitere Systeme (s. Anlage 4). Es werden nur diejenigen Daten übergeben, die für die Zweckbestimmung des Zielsystems erforderlich sind.

11 Weiterentwicklung des Forschungsinformationssystems (Releases)

Das System Pure wird ständig weiterentwickelt. Etwa dreimal pro Jahr wird eine aktualisierte Version als sog. Major Release herausgebracht, die der LUH im Rahmen des mit Elsevier geschlossenen Vertrages zur Verfügung steht. Diese Weiterentwicklungen betreffen fachliche Prozesse, die der Softwareanbieter aus den Anregungen aller Kunden aufnimmt und in die Software einfließen lässt. Außerdem werden monatlich Minor Releases zur Verfügung gestellt, die insbesondere Bug fixes enthalten. Entsprechend sind die Dienststelle und die Personalräte sich darüber einig, dass das Forschungsinformationssystem, wie es an der LUH implementiert ist, einer stetigen Entwicklung unterliegen wird, um die Anpassung an neue oder veränderte inhaltliche Bedarfe, rechtliche Vorgaben und/oder Prozessabläufe zu gewährleisten.

Die für den FIS-Betrieb zuständige Stelle kann Änderungen, die ausschließlich dazu dienen, den technischen Betrieb sicherzustellen oder abzusichern (insbesondere Fehlerbehebung im Rahmen des sog. „Bug Fixing“ oder vergleichbare Maßnahmen) jederzeit durchführen. Erweiterungen der Funktionalität des Forschungsinformationssystems sind vorher durch die Dienststelle mit dem Datenschutzbeauftragten und den Personalräten abzustimmen, soweit hierfür eine Verarbeitung personenbezogener Daten erforderlich ist. Entsprechend vereinbarte Änderungen werden in den Anlagen dieser Dienstvereinbarung und der Beschreibung der Verarbeitungstätigkeit gem. Art. 30 DSGVO dokumentiert.

12 Anlagenübersicht

Anlage 1	Fachkonzept
Anlage 2	Systembeschreibung „Pure-Hosting für die LUH“
Anlage 3	Datenkatalog
Anlage 4	Übersicht Quell- und Zielsysteme sowie Datenweitergabe
Anlage 5	Schnittstellenbeschreibung SAP-HCM-FIS
Anlage 6	Schnittstellenbeschreibung SAP-FM-FIS
Anlage 7	Datenschutz- und Löschkonzept
Anlage 8	Rechte- und Rollenkonzept
Anlage 9	Berichtskonzept
Anlage 10	Support- und Schulungskonzept

Anlage 11	Meldung der Verarbeitungstätigkeit gem. Art. 30 DSGVO
-----------	---

13 Inkrafttreten

Durch den Abschluss dieser Dienstvereinbarung und durch die jeweils erteilte Zustimmung des Personalrates zur Produktivsetzung des Forschungsinformationssystems gilt die Mitbestimmung gem. NPersVG - im Hinblick auf Neueinführung, Änderungen und Erweiterungen – nicht als verbraucht. Alle in dieser Dienstvereinbarung bzw. der Anlagenübersicht aufgeführten Anlagen sind Bestandteil dieser Vereinbarung. Sie werden regelmäßig aktualisiert und mit Versionsnummer und Erst- bzw. Änderungsdatum dieser Dienstvereinbarung beigefügt. Erweiterungen der Funktionalität des Forschungsinformationssystems sind vorher durch die Dienststelle mit dem Datenschutzbeauftragten und den Personalräten zu regeln.

Diese Dienstvereinbarung mit Anlagen tritt am 01.11.2019 in Kraft. Sie kann einseitig unter Einhaltung einer Kündigungsfrist von 4 Monaten, frühestens jedoch zum 31.12.2020, gekündigt werden. Sollten einzelne Bestimmungen dieser Vereinbarung insbesondere wegen Verstoßes gegen § 82 NPersVG, nichtig sein oder werden, so berührt dies nicht die Gültigkeit der übrigen Bestimmungen. Anstelle der unwirksamen Bestimmungen, oder zur Ausfüllung eventueller Lücken der Vereinbarung soll eine angemessene Regelung in Kraft treten, die dem am Nächsten kommt, was die Parteien nach ihrer Zwecksetzung gewollt haben. Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform. Im Übrigen gilt § 78 Abs. 4 NPersVG.

Die Dienstvereinbarung ist allen Beschäftigten in geeigneter Weise bekannt zu machen.

Hannover, den 16.10.2019

Hannover, den 23.10.2019

Leibniz Universität Hannover
Das Präsidium

Leibniz Universität Hannover
Personalrat

gez. Prof. Dr. Volker Epping
Präsident

gez. Elli Grube
Vorsitzende

Die nachfolgende Dienstvereinbarung, unterzeichnet vom Präsidium der Gottfried Wilhelm Leibniz Universität Hannover am 21.08.2019 sowie vom Personalrat der Gottfried Wilhelm Leibniz Universität Hannover am 04.09.2019, ist abgeschlossen worden. Sie trat zum 01.10.2019 in Kraft.

**Dienstvereinbarung gem. § 78 NPersVG
zur Einführung eines Systems zur elektronischen Probandenverwaltung
bei der Stabsstelle Arbeitssicherheit
an der Leibniz Universität Hannover**

**zwischen
der Leibniz Universität Hannover,**

**und
dem Personalrat der Leibniz Universität Hannover**

1. Präambel

Sowohl für die Beschäftigten als auch für die Studierenden ist seitens der Leibniz Universität Hannover (LUH) die betriebsärztliche Versorgung zu gewährleisten. Aufgrund der Anzahl der Personen kann ein Probandenmanagement nur mittels einer digitalen Aktenführung sinnvoll durchgeführt werden. Hierfür ist eine Software einzusetzen, die die Behandlungsplanung und Evaluation unterstützt.

2. Ziel und Zweckbestimmung

Die Pflicht der Dokumentation von Probandenakten ergibt sich aus der Berufsordnung der Ärztekammer Niedersachsen.

In dieser Dienstvereinbarung wird der Rahmen zur angemessenen und sinnvollen Nutzung elektronischer Probandenakten bei der betriebsärztlichen Abteilung der Stabsstelle Arbeitssicherheit der LUH geregelt und im Besonderen der Schutz der personenbezogenen Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff sichergestellt.

Bestandteile der elektronischen Probandenakte sind die Behandlungsplanung, anamnestische Daten und Aufzeichnungen zum Behandlungsverlauf. Darüber hinaus werden mit den erhobenen Daten keine Adressdatenbanken oder andere Sammlungen mit Personendaten angelegt.

Alle erfassten Daten werden ausschließlich zur Vorsorge, Untersuchung und Beratung der Probanden genutzt und nicht an andere Personen oder Einrichtungen weitergegeben.

Diese Dienstvereinbarung wird gem. § 59, 60, 64, 66, und 67 i.V.m. § 78 NPersVG (Niedersächsisches Personalvertretungsgesetz) geschlossen. Für die Verarbeitung personenbezogener Daten bei der Leibniz Universität gelten die Bestimmungen der EU-Datenschutzgrundverordnung (EU-DSGVO), des Niedersächsischen Datenschutzgesetzes (NDSG) i. V. m. den §§ 88 ff. des Niedersächsischen Beamtengesetzes (NBG) und den Datenschutzrichtlinien der EU.

3. Geltungsbereich

Diese Vereinbarung gilt für alle Beschäftigten der LUH.

4. Systembeschreibung, Leistungsumfang

Das Patientenmanagement der Firma CompuGroup Medical Deutschland AG ist eine Client-/Server-basierte Anwendung. Der Server und die Datenbank befinden sich auf einem separaten Hardware-Server im Serverraum des Sachgebietes 12 (luK). Die Client-Anwendung ist auf den APCs der betriebsärztlichen

Abteilung der Stabsstelle Arbeitssicherheit installiert. Die Übertragung von Eingaben und allen in der Anwendung vorgehaltenen Daten erfolgt TLS-verschlüsselt, die Authentifizierung erfolgt per Smart-Card und Client-Zertifikat. Der Zugang zur Anwendung ist über individuelle Accounts gewährleistet und über die Rollenzuordnung mit unterschiedlichen Rechten versehen (Anlage 5). Zugangsdaten für bestehende und neue Benutzerinnen und Benutzer werden von der zentralen Anwendungsadministration angelegt und verwaltet. Die zentrale Anwendungsadministration obliegt der leitenden Betriebsärztin/dem leitenden Betriebsarzt und der von ihr oder ihm benannten Stellvertretung.

Ein Backup der Datenbank und des Serversystems erfolgt verschlüsselt über den Backup-Dienst des LUIS. Für die Systemadministration sind im Sachgebiet 12 max. drei Personen namentlich festgelegt.

5. Schutz der Persönlichkeitsrechte, Datenschutz, Löschfristen

Alle Benutzerinnen und Benutzer dieser Software (betriebsärztliche Abteilung) werden zur Wahrung der Schweigepflicht verpflichtet.

Die Probanden haben jederzeit die Möglichkeit der Einsichtnahme in Ihre ärztliche Akte.

Daten im Sinne dieser Dienstvereinbarung dürfen ausschließlich für die hier vereinbarten Zwecke verarbeitet werden. Die zum Erreichen der Zweckbestimmung dieser Dienstvereinbarung erforderlichen Personendaten die erhoben, verarbeitet und genutzt werden, sind in Anlage 1 abschließend aufgeführt und dokumentiert.

Die datenschutzrechtlichen Bestimmungen werden eingehalten. Darüber hinaus verpflichtet sich die LUH zu einem Umgang mit persönlichen Daten, der dem Grundsatz der unbedingten Erforderlichkeit der Datenerhebung, -verarbeitung und -nutzung folgt.

Nach Ablauf der ärztlichen Aufbewahrungsfristen erfolgt eine Löschung der Probandenakten gemäß den Anforderungen der EU-DSGVO.

6. Berechtigungskonzept - Zugriffsbestimmungen

Eine volle Zugriffsberechtigung auf die Fallakten, inklusive der Gesprächsdokumentation, haben nur die Betriebsärzte.

Die Hardwareadministration darf nicht auf die Daten zugreifen. Eine Beschreibung des Rechtekonzeptes ist in Anlage 5 dargestellt.

7. Berichte und Auswertungen

Die Anwendung verfügt über Druck- und Exportfunktionen. Die sichere Verwahrung dieser so ausgegebenen Daten wird von der betriebsärztlichen Abteilung gewährleistet. Eine Weitergabe der Daten erfolgt ausschließlich an die Probanden.

Zu Berichtszwecken und zur Qualitätssicherung werden Auswertungen und Evaluationen anonymisiert und nicht personenbeziehbar durchgeführt (z.B. Impfstoff- und Fristenmanagement).

Bei Änderungen des Verwendungszwecks und des Umfangs der Auswertungen ist der Personalrat vorab zu unterrichten.

Auswertungen der Protokolldateien dienen ausschließlich der Gewährleistung der Betriebs- und Systemsicherheit.

Die Software darf nicht zur Überwachung des Verhaltens und der Leistung der Beschäftigten genutzt werden.

8. Schnittstellen

In die Probandenakten werden Messwerte aus gerätespezifischen Anwendungen importiert. Die Geräte werden ausschließlich über USB Ports angeschlossen. Eine Auflistung der Messgeräte findet sich in Anlage 2.

Eine Verknüpfung des Probandenmanagements mit weiterer Software oder anderen Datenbanken erfolgt nicht.

9. Qualifizierung

Die Beschäftigten der betriebsärztlichen Abteilung werden entsprechend für die Bearbeitung der Software geschult.

10. Rechte der Personalvertretung

Der Personalrat hat jederzeit das Recht, Einblick in das System zu nehmen, um die Funktionsweise zu überprüfen, ohne dabei auf die Inhalte der ärztlichen Akte Einsicht zu erhalten.

11. Schlussbestimmungen, Inkrafttreten, Kündigung

Sofern einzelne Bestimmungen dieser Dienstvereinbarung unwirksam sind oder werden, wird davon die Wirksamkeit der übrigen Bestimmungen nicht berührt. Sollte den Vertragsschließenden dieser Dienstvereinbarung eine eventuelle Unwirksamkeit bekannt werden, verpflichten sie sich, schnellstmöglich eine neue Regelung zu treffen, die dem gewollten Sinn und Zweck der unwirksamen Bestimmung soweit wie möglich entspricht. Sollten Tatbestände durch diese Dienstvereinbarung nicht geregelt sein, die den Vertragsschließenden dieser Dienstvereinbarung bekannt werden, so verpflichten sie sich, umgehend eine Regelung ergänzend zu vereinbaren, die den Grundsätzen dieser Dienstvereinbarung entspricht.

Das gilt auch, falls durch Softwareupdates wesentliche Bestandteile der Probandenverwaltung modifiziert oder durch den Einsatz zusätzlicher Module die in dieser Dienstvereinbarung geregelte Funktionen verändert oder ergänzt werden.

Diese Dienstvereinbarung tritt mit ihrer Unterzeichnung in Kraft. Alle in dieser Dienstvereinbarung bzw. der Anlageübersicht angeführten Anlagen sind Bestandteil dieser Vereinbarung.

Sie kann beiderseitig unter Einhaltung einer Kündigungsfrist von 4 Monaten gekündigt werden. Nach dem Auslaufen der Dienstvereinbarung ist der Einsatz des Systems / der Software unzulässig und sofort zu stoppen.

Ergänzungen und Änderungen sind jederzeit im beiderseitigen Einvernehmen möglich, sie bedürfen der Schriftform.

Hannover, den 21.08.2019

Hannover, den 04.09.2019

Leibniz Universität Hannover
Prof. Dr. iur. Volker Epping
Präsident

Leibniz Universität Hannover
Elvira Grube
Vorsitzende des Personalrats

Anlagen:

Anlage 1 – Softwarebeschreibung

Die Anlage 1 zu dieser Dienstvereinbarung kann bei Herrn Dietrich im Sachgebiet 21 eingesehen werden.

Anlage 2 – Auflistung der angeschlossenen Messgeräte

Anlage 3 – Darstellung einer Verarbeitungstätigkeit nach Art. 30

Anlage I – Dokumentationshilfe für die Pflichten nach Art. 5 Abs. 2 DSGVO

Anlage II – Dokumentation der technischen und organisatorischen Maßnahmen i.S.v. Art. 32 DSGVO

Anlage 4 – Probandeninformation zum Datenschutz

Anlage 5 – Einführung eines Systems zur elektronischen Probandenverwaltung

Anlage 2 – Auflistung der angeschlossenen Messgeräte

Auflistung der Geräte, die per USB an das System angeschlossen werden.

1. Sehtestgerät „Optovist II“ von Fa. Vistec
2. Ton-Audiometer „CAS 1001 K“ von Fa. Audio-Ton
3. Spirometer „Pneumotrac-USB“ von Fa. Vitalograph



An den Datenschutzbeauftragten:

Ass. iur. Simon Graupe, LL.M. (DS)

- hier: 20001220 -

datenschutz@uni-hannover.de

**Az.: DS -
(wird ausgefüllt)**

**Darstellung einer Verarbeitungstätigkeit nach Art. 30 DSGVO Name
des Verfahrens:**

Klicken Sie hier, um Text einzugeben.		
<input checked="" type="checkbox"/> Ersterfassung	<input type="checkbox"/> Änderung	<input type="checkbox"/> Löschung

1. Zwecke der Verarbeitung

Verarbeitung von Probandendaten zur Vorsorge, Untersuchung und Beratung (Einsatz und Nutzung von Probandendaten).

2. Kategorien betroffener Personen und Kategorien personenbezogener Daten

Lfd. Nr.	Personenkreis	Datenkategorie
1	Probanden: Beschäftigte	Name, Vorname, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Anschrift, Tätigkeiten, Gesundheitsdaten
2	Probanden: Studierende	Name, Vorname, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Anschrift, Tätigkeiten, Gesundheitsdaten

3. Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden einschließlich Empfängern in Drittländern oder internationalen Organisationen

a) Hochschulinterne Empfänger

Offengelegte Daten (Ifd. Nr. aus 2)	Hochschulinterne Empfänger
	Personal der Betriebsärztlichen Abteilung
	Personalabteilung im Rahmen der Verpflichtung Vorsorgebescheinigungen auszustellen (Verordnungsgrundlage: ArbMedVV)
	Vorgesetzte, BEM-Mitglieder, Personalrat: Eignungsbescheinigungen werden an den Probanden zur möglichen Weiterleitung ausgegeben. Eine direkte Weitergabe von Eignungsbescheinigungen oder mündlichen Auskünften erfolgt nur mit Einwilligungserklärung und Schweigepflichtentbindung.

b) Hochschulexterne Empfänger innerhalb der EU

Offengelegte Daten (Ifd. Nr. aus 2)	Hochschulexterne Empfänger innerhalb der EU
	Ärztliches, medizinisches Personal, Berufsgenossenschaften, Unfallversicherungsträger, Gesundheitsdaten nur nach Schweigepflichtentbindung, ggf. bestehen Informationspflichten

c) Hochschulexterne Empfänger außerhalb der EU

Offengelegte Daten (Ifd. Nr. aus 2)	Hochschulexterne Empfänger außerhalb der EU (Drittländer und internationale Organisationen) in Fällen des Art. 49 Abs. 1 Unterabs. 2 DSGVO einschließlich der Dokumentierung der geeigneten Garantien
	Gesundheitszertifikate für Dienstreisen werden dem Probanden zur Weiterleitung ausgehändigt.

4. Fristen für die Löschung von Daten (bei unterschiedlichen Löschfristen laufende Nummer der Datenkategorie angeben oder Verweis auf das Löschkonzept)

Es gelten die Berufsordnung (§ 10 BO der ÄKWL), der Bundesmantelvertrag-Ärzte (§ 57 BMV-Ä), das Patientenrechtegesetz (§ 630f Bürgerliches Gesetzbuch), die Strahlenschutzverordnung (StrlSchV), die Röntgenschutzverordnung (RöV), die Arbeitsmedizinische Regel AMR 6.1.

AMR 6.1: mind. 40 Jahre nach der letzten Vorsorge, soweit die Tätigkeiten erbgutverändernde oder krebserzeugende Stoffe betreffen oder bei Zubereitungen der Kategorie K1 oder K2 i. S. d.

Gefahrenstoffverordnung oder bei Tätigkeiten die zu Berufskrankheiten führen können; ist der Zeitpunkt der letzten Gefährdung bekannt spätestens am 31.12 des 40. Jahres oder 10 Jahre nach dem Tod des Beschäftigten; 10 Jahre nach Abschluss der Behandlung i. S. d. Berufsordnung.

Strahlenschutzgesetz § 79: Aufbewahrung bis zu. LJ, jedoch bis mindestens 30 Jahre nach Beendigung der Wahrnehmung von Aufgaben als beruflich exponierte Person, spätestens bis 100 Jahre nach der Geburt der überwachten Person.

5. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO (grob skizzieren oder Anlage II beifügen und auf diese verweisen)

Die betriebsärztliche Abteilung setzt technische und organisatorische Sicherheitsmaßnahmen nach Art. 32 EU-DSGVO ein, um die Daten der Probanden gegen zufällige oder vorsätzliche Manipulation zu schützen. Die eingesetzten Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert.

6. Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten.

a) Beginn der Verarbeitung

Die Verarbeitung findet bereits statt.

Die Verarbeitung soll ab _____ erfolgen.

b) Rechtsgrundlage der Verarbeitung (Art. 5 Abs. 1 a i.V.m. Art. 6 DSGVO)

Die Datenverarbeitung erfolgt aufgrund folgender Rechtsgrundlagen (bei mehreren Rechtsgrundlagen bitte manuell nach Datenkategorie spezifizieren):

Arbeitssicherheitsgesetz, Verordnung zur arbeitsmedizinischen Vorsorge, Strahlenschutzgesetz und deren Verordnungen, Gefahrstoffverordnung, Sozialgesetzbuch VII und IX, arbeitsrechtliche Grundlagen des Arbeitgebers, TV-L § 3 (5), Jugendarbeitsschutzgesetz.

c) Rechtsgrundlage für die Übermittlung von Daten externe Empfänger

Datenverarbeitung durch Auftragsverarbeiter nach Art. 28f. DSGVO

Name und Anschrift des Auftragsverarbeiters:
 Die Auftragsverarbeitung ist durch einen schriftlichen Vertrag, der Regelungen zu Aufträgen, Weisungen zu technischen und organisatorischen Maßnahmen und die Zulassung von Unterauftragsverhältnissen enthält, geregelt. Der Vertrag wurde dem Datenschutzbeauftragten zur Prüfung vorgelegt.

Datenübermittlung an Dritte innerhalb der EU (Ziffer 3.b des Verzeichnisses):

Zweck der Übermittlung:
Rechtsgrundlage für die Übermittlung:
Schnittstelle für die Übermittlung:
Häufigkeit der Übermittlung:
Bei Übermittlung an unterschiedliche Stellen bitte Antwortfelder vor dem Eintrag entsprechend kopieren.

Datenübermittlung an Dritte außerhalb der EU (Ziffer 3.c des Verzeichnisses):

Zweck der Übermittlung:
Rechtsgrundlage für die Übermittlung:
Schnittstelle für die Übermittlung:
Häufigkeit der Übermittlung:
Bei Übermittlung an unterschiedliche Stellen bitte Antwortfelder vor dem Eintrag entsprechend kopieren.

d) Verfahren zur Löschung der Daten (gemäß Ziffer 4 des Verarbeitungsverzeichnisses)

Die Löschung der Daten erfolgt manuell / automatisch wie folgt:

Manuell.

e) Transparenz: Sind Form und Umfang der Verarbeitung für Betroffene erkennbar?

Form der Verarbeitung (mehrere Angaben möglich):

Die Verarbeitung erfolgt schriftlich.

Die Verarbeitung erfolgt mit Hilfe automatisierter Verfahren.

Die Verarbeitung erfolgt formlos (z.B. mündlich oder fernmündlich).

Die Informationspflichten nach Art 12 DSGVO sind bekannt und werden gewährleistet.

7. Für die Verarbeitungstätigkeit innerhalb der Leibniz Universität verantwortliche Stelle (Einrichtung / Fakultät/ Institut)

Einrichtung / Fakultät / Institut:

Leibniz Universität Hannover, Stabsstelle Arbeitssicherheit, Welfengarten 1, Hannover

Ansprechpartner für Rückfragen (Name, Telefonnummer): Dr. Ellen Aumüller, Betriebsärztin

8. Regelmäßige Überprüfung

Die Aktualität der Verfahrensbeschreibung wird

jährlich

_____ (anderer Prüfturnus)

überprüft.

Erster Prüftermin (1 Jahr nach Meldung oder bei gravierenden Änderungen): Klicken Sie hier, um ein Datum einzugeben.

_____ Datum und Unterschrift Verantwortlicher (Instituts-/Einrichtungsleitung/Dezernent/Sachgebietsleitung)

Kontrolle durchgeführt, keinen Handlungsbedarf festgestellt

Datum	Name								

Bearbeitungsvermerke (wird durch den Datenschutzbeauftragten ausgefüllt): 1) Weiterer Handlungsbedarf?

2) Wv. gemäß nächstem Prüftermin



Anlage I – Dokumentationshilfe für die Pflichten nach Art. 5 Abs. 2 DSGVO

Name der Verarbeitungstätigkeit:

Erhebung und Speicherung von Gesundheitsdaten.

A.1. Zusätzliche Angaben bei elektronischer Datenverarbeitung

a. Eingesetzte Hardware

1 Server im Serverraum von Sachgebiet 12 und Backup im Backupdienst des LUIS 2 Desktop-PCs und ein Laptop als Clients in der betriebsärztlichen Abteilung

b. Eingesetzte Software

CMG ISIS MED,
Outlook, Thunderbird,
CRM travel.DOC (reisemedizinisches Beratungssystem mit länderspezifischen Fachinformationen)

c. Datenminimierung durch datenschutzfreundliche Voreinstellungen:

Die Voreinstellungen sind so konfiguriert, dass möglichst wenige Daten gespeichert werden.

A.2. Risikoanalyse

a. Festlegung des Schutzbedarfes nach Schutzstufenkonzept

Lfd. Nr.	Datenkategorie	Es handelt sich um besonders sensible Daten nach Art. 9 DSGVO	Ungefähre Anzahl der Betroffenen	Festlegung des Schutzbedarfes (normal, hoch, sehr hoch)
1	Name, Vorname, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Anschrift, Tätigkeiten, Gesundheitsdaten	Ja	Ca. 5000 Beschäftigte und ca. 30000 Studierende	Sehr hoch.
2				
3				

In der Gesamtschau wird für das Verfahren ein sehr hoher Schutzbedarf festgelegt.

b. Für das Verfahren relevante Risiken:

<u>Risiko</u>	<u>Bedrohung</u>	<u>Potentielle Schwachstellen</u>	<u>Eintrittswahrscheinlichkeit (gering, normal, hoch, sehr hoch)</u>
Feuer	Vernichtung	Holzschränke	gering
Diebstahl	Verlust	Holzschränke, mobiles Endgerät	gering
	Veränderung		
	Unbefugte Offenlegung		
Einbruch	Unbefugter Zugang	Türschlösser und Schrankschlösser	normal
	(bitte ggf. weitere als relevant identifizierte Risiken ergänzen)		

A.3. Erforderlichkeit einer Datenschutz-Folgenabschätzung nach Art 35 DSGVO

Eine Datenschutz-Folgenabschätzung ist nach Art. 35 DSGVO erforderlich.

Die Datenschutz-Folgenabschätzung wurde am _____ unter dem Aktenzeichen _____ durchgeführt.

A.4. Technische und organisatorische Maßnahmen (Datensicherheitsmaßnahmen)

Dokumentation gem. Anlage II

Weitere technische und organisatorische Maßnahmen?

Eigener Server für die Arbeitsmedizin. Server und Clients sind in einem separaten, extra gesicherten Netzbereich organisiert. Zugriff durch Administrator nur zur Hardwarepflege möglich, ohne Zugriff auf Gesundheitsdaten.

A.5. Bewertung der Maßnahmen im Verhältnis zum Risiko

Ist das durch die technisch organisatorischen Maßnahmen gewährleistete Schutzniveau gegenüber dem Risiko angemessen?

ja nein

Anlage II – Dokumentation der technischen und organisatorischen Maßnahmen i.S.v. Art. 32 DSGVO

Name der Verarbeitungstätigkeit:

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- | | |
|--|---|
| <input type="checkbox"/> Alarmanlage | <input type="checkbox"/> Absicherung von Gebäudeschächten |
| <input type="checkbox"/> Automatisches Zugangskontrollsystem | <input checked="" type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input type="checkbox"/> Schließsystem mit Codesperre | <input type="checkbox"/> Manuelles Schließsystem |
| <input type="checkbox"/> Biometrische Zugangssperren | <input type="checkbox"/> Videoüberwachung der Zugänge |
| <input type="checkbox"/> Lichtschranken / Bewegungsmelder | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen |
| <input checked="" type="checkbox"/> Passwortvergabe | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| <input type="checkbox"/> Gehäuseverriegelungen | <input type="checkbox"/> Einsatz von VPN-Technologie |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input type="checkbox"/> Verschlüsselung von mobilen Datenträgern |
| <input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten | <input type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |

- | | |
|---|---|
| <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software | <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input checked="" type="checkbox"/> Einsatz einer Hardware-Firewall | <input checked="" type="checkbox"/> Einsatz einer Software-Firewall |

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input checked="" type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input type="checkbox"/> Protokollierung der Vernichtung |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern | <input type="checkbox"/> Pseudonymisierung personenbezogener Daten, sobald der Zweck dies zulässt |

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- | | |
|---|---|
| <input type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen | |

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- | | |
|--|--|
| <input type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <input type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | |

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- | | |
|--|--|
| <input type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <input type="checkbox"/> vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) | <input type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis |
| <input type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt | <input type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <input type="checkbox"/> Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | <input type="checkbox"/> laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |
| <input type="checkbox"/> Vertragsstrafen bei Verstößen | |

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input type="checkbox"/> Klimaanlage in Serverräumen |
| <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input checked="" type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recoverykonzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung | <input checked="" type="checkbox"/> Erstellen eines Notfallplans |

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- In Hochwassergebieten: Serverräume über der Wassergrenze

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

**Stabsstelle Arbeitssicherheit**

Leibniz Universität Hannover

Information zum Datenschutz: Juni 2019

PROBANDENINFORMATION ZUM DATENSCHUTZ

Nach der EU-Datenschutz-Grundverordnung (DSGVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck die betriebsärztliche Abteilung der Leibniz Universität Hannover Daten erhebt, speichert oder weiterleitet. Der Information können Sie auch entnehmen, welche Rechte Sie in puncto Datenschutz haben.

Um die betriebsärztliche Betreuung zu sichern, müssen Dokumentations- und Aufbewahrungspflichten erfüllt werden, die eine Datenerhebung und Datenspeicherung erfordern (z. B. Personaldaten, Anamnesen, allgemeine Angaben zum Beratungsanliegen, Gesprächsdokumentationen, Verlaufsdocumentationen etc.). Dabei werden selbstverständlich die jeweils aktuellen datenschutzrechtlichen Vorgaben der EU Datenschutzgrundverordnung (EU-DSGVO) und des Landesdatenschutzgesetzes (NDSG) beachtet.

Sämtliche Informationen sowie Angaben über Ihre Identität und die Tatsache Ihrer Beratung unterliegen der Schweigepflicht¹. Inhalte Ihres Gesprächs mit Ihrem Betriebsarzt bzw. Ihrer Betriebsärztin werden streng vertraulich behandelt. Die Beschäftigten der betriebsärztlichen Abteilung vertreten sich gegenseitig in Urlauben und Krankheitsfällen. Zu diesem Zwecke nehmen sie auch Einsicht in die Dokumentation.

1. VERANTWORTLICHKEIT FÜR DIE DATENVERARBEITUNG

Verantwortlich für die Datenverarbeitung ist:

Leibniz Universität Hannover
Stabsstelle Arbeitssicherheit

Welfengarten 1, 30167 Hannover

Sie erreichen die/den zuständige/n Datenschutzbeauftragte/n unter:

Leibniz Universität Hannover

- Datenschutzbeauftragter -

Königsworther Platz 1, 30167 Hannover

Tel.: + 0511 762 8132 datenschutz@uni-hannover.de

2. ZWECK UND ART DER DATENVERARBEITUNG

Die Datenverarbeitung erfolgt in dem Umfang, der notwendig ist (Zweckbindung/Datenminimierung), um den rechtlich verankerten Aufgaben eines Betriebsarztes gerecht zu werden.

Hierzu verarbeiten wir Ihre personenbezogenen Daten, insbesondere Ihre Gesundheitsdaten. Dazu zählen Anamnesen, Diagnosen und Befunde, die wir oder andere Ärzte erheben. Zu diesen Zwecken können uns auch andere Ärzte oder Psychotherapeuten, bei denen Sie in Behandlung sind, Daten zur Verfügung stellen (z.B. in Arztbriefen).

Die Erhebung von Gesundheitsdaten ist Voraussetzung für Ihre arbeitsmedizinische Vorsorge bzw. Einstellungs- und Eignungsuntersuchung. Werden die notwendigen Informationen nicht bereitgestellt, kann die Vorsorge bzw. Untersuchung nicht erfolgen.

3. EMPFÄNGER IHRER DATEN

Wir übermitteln Ihre personenbezogenen Daten nur dann an Dritte, z.B. andere Ärzte, Unfallversicherungsträger, wenn dies gesetzlich erlaubt ist oder Sie eingewilligt haben.

Als externen Dienstleister zur Erstellung von Laborbefunden wird das MVZ Labor Limbach eingesetzt. Das Labor wird von einem Berufsheimnisträger geführt, der der gesetzlichen Schweigepflicht unterfällt. Die Übermittlung ist gestützt auf Art. 9 Abs. 2 lit. h) DSGVO.

Die Übermittlung erfolgt überwiegend zur Klärung von medizinischen und sich aus Ihrem Versicherungsverhältnis ergebenden Fragen.

Gemäß der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) sind wir verpflichtet, dem Arbeitgeber eine Bescheinigung über Ihre Vorsorge mit den Beschäftigtenstammdaten, dem Datum, dem Anlass der Vorsorge nach ArbMedVV und dem Termin der nächsten arbeitsmedizinischen Vorsorge auszustellen.

Ergebnisse von Eignungsuntersuchungen für den Arbeitgeber erhalten Sie persönlich zur möglichen Weiterleitung.

4. SPEICHERUNG IHRER DATEN

Die Daten werden entsprechend rechtlicher Vorgaben für die Aufbewahrungsfristen gespeichert, danach wird eine Löschung durchgeführt.

Die Daten sind mindestens 10 Jahre nach Abschluss einer Beratung aufzubewahren. Auf Grund anderer

Vorschriften können sich Aufbewahrungsfristen bis zu 40 Jahren ergeben, z.B. bei der arbeitsmedizinischen Vorsorge wegen Tätigkeiten mit krebserzeugenden oder erbgutverändernden Stoffen oder bei Tätigkeiten, die zu Berufskrankheiten führen können.

Die Daten werden auf einem Server der Leibniz Universität Hannover, der AES-verschlüsselt ist gespeichert, die Datenfelder sind verschleiert, d.h. die Administratoren können die Inhalte nicht einsehen. Die Wartung der Software wird vom Sachgebiet 12 durchgeführt. Die Übertragung von Eingaben und allen in der Anwendung vorgehaltenen Daten erfolgt TLS-verschlüsselt. Der Zugang zur Anwendung für die betriebsärztliche Abteilung ist über individuelle Accounts gewährleistet und über die Rollenzuordnung mit unterschiedlichen Rechten versehen. Es haben ausschließlich die Mitarbeiter und Mitarbeiterinnen der betriebsärztlichen Abteilung Zugang zu den Daten.

5. IHRE RECHTE

Sie haben das Recht, über die Sie betreffenden personenbezogenen Daten und den Zweck der Datenspeicherung Auskunft zu erhalten.

Sie haben das Recht, die Einwilligung zur Verarbeitung personenbezogener Daten jederzeit zu widerrufen. Durch den Widerruf wird jedoch nicht die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt. Auch können Sie die Berichtigung unrichtiger Daten verlangen.

Darüber hinaus steht Ihnen unter bestimmten Voraussetzungen das Recht auf Löschung von Daten, das Recht auf Einschränkung der Datenverarbeitung sowie das Recht auf Datenübertragbarkeit zu, sofern die oben erwähnten berufs- und zivilrechtlichen vorgeschriebenen Dokumentations- und Aufbewahrungspflichten dem nicht höherrangig entgegenstehen. Es besteht vor Ablauf der gesetzlichen Aufbewahrungsfristen kein Anspruch auf Löschung bzw. Sperrung von personenbezogenen Daten.

Sie haben das Recht, sich bei der zuständigen Aufsichtsbehörde für den Datenschutz zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Die Anschrift der für uns zuständigen Aufsichtsbehörde lautet:

Landesbeauftragte für den Datenschutz Niedersachsen.

Prinzenstr. 5, 30159 Hannover

6. RECHTLICHE GRUNDLAGEN

Rechtsgrundlage für die Verarbeitung Ihrer Daten ist Artikel 9 Absatz 2 lit. h) DSGVO in Verbindung mit § 17 Abs. 1 Nr. 3 NDSG. Sollten Sie Fragen haben, können Sie sich gern an uns wenden.



Anlage 5 zur Dienstvereinbarung zur Einführung eines Systems zur elektronischen Probandenverwaltung

Berechtigungskonzept Probandenverwaltung Zur Dienstvereinbarung Stabsstelle Arbeitssicherheit, Abschnitt Arbeitsmedizin

Rollen

Es findet eine strikte Hard-/Softwaretrennung statt.

Die Administration der Hardware (Server und APCs) erfolgt durch drei definierte Mitarbeiter des Sachgebietes 12 (IuK).

Die Administration der Anwendung erfolgt durch die Betriebsärztin / den Betriebsarzt.

1. Rolle: Anwender

- Zweck/wofür: Nutzung der Clients
- wer: Mitarbeiter des Abschnitts Arbeitsmedizin
- Rechte: Eintragungen in die Datenbank, Anlegen von Probandenakten, Pflege der Daten

2. Rolle: Anwendender Arzt

- Zweck/wofür: Nutzung der Clients
- wer: Betriebsarzt / Betriebsärztin
- Rechte: erweiterte Eintragungen in die Datenbank, Anlegen von Probandenakten, Pflege der Daten

3. Rolle: Anwendungsadministrator

- Zweck/wofür: Verwaltung von Anwenderkonten.
- wer: leitende Betriebsärztin / leitender Betriebsarzt
- Rechte: Anlegen von Anwendern, Vergabe von Rechten innerhalb der Anwendung, Eintragungen in die Datenbank, Anlegen von Probandenakten, Pflege der Daten

4. Rolle: Hardwareadministrator

- Zweck/wofür: Verwaltung von Server und APCs.
- wer: max. 3 Mitarbeiter in Sachgebiet 12 (IuK) Organisationseinheit die Verwaltungshoheit haben.
- Rechte: Bereitstellung und Pflege von IT-Hardware für die Mitarbeiter der betriebsärztlichen Abteilung in der Stabsstelle Arbeitssicherheit. Konfiguration der Netzwerkinfrastruktur.

Aktion		Rollen Verwaltung		Benutzer	Benutzer
		Hardware administrator	Anwendungs administrator	Anwendend Arzt / Betriebsarzt	Anwende
Erheben	Persönliche Daten		X	X	X
Erheben/ Anzeigen	Gesprächsprotokolldaten		X	X	
Suchen	Gespeicherte Daten einer Person		X	X	X
Anzeigen	Anzeigen der Daten einer Person		X	X	X
Ändern	Ändern der Kontaktdaten von einer Person		X	X	X
	Persönliches Kontopasswort für angeschlossene Dienst ändern		X	X	X
Löschen	Löschen von Daten einer Person		X	X	X
Zufügen	Zufügen der Berechtigungen durch Zuweisung der Rollen		X		
	Beschaffung und Bereitstellung des Servers, der APCs und Konfiguration der Netzwerkinfrastruktur	X			

Die nachfolgende Dienstvereinbarung, unterzeichnet vom Präsidenten der Gottfried Wilhelm Leibniz Universität Hannover am 08.08.2019 sowie vom Personalrat der Gottfried Wilhelm Leibniz Universität Hannover am 14.08.2019, ist abgeschlossen worden. Sie tritt zum 15.08.2019 in Kraft.

**Dienstvereinbarung über die Einführung und Anwendung des
Veranstaltungsmanagementsystems „Antrago“**

an der Gottfried Wilhelm Leibniz Universität Hannover

**zwischen der Leibniz Universität Hannover und
dem Personalrat der Leibniz Universität Hannover
in der Fassung vom 02.08.2019**

Inhaltsverzeichnis

1	Präambel
2	Gegenstand
3	Geltungsbereich
4	Systembeschreibung, Leistungsumfang
5	Ziel und Zweckbestimmung des Veranstaltungsmanagementsystems
6	Schutz der Persönlichkeitsrechte, Datenschutz und Löschkonzept
7	Berechtigungskonzept
8	Berichte und Auswertungen
9	Leistungs- und Verhaltenskontrolle
10	Schnittstellen/Datenexport, -import
11	Rechte der Beschäftigten, Qualifizierung
12	Anlagenübersicht
13	Schlussbestimmungen, Inkrafttreten, Kündigung

1. Präambel

Die Leibniz Universität Hannover führt die Software ANTRAGO der Firma RR Software GmbH als Veranstaltungsmanagementsystem ein. Das Veranstaltungsmanagementsystem ANTRAGO schafft die technischen Voraussetzungen für die Planung und Verwaltung von Qualifizierungsangeboten, die nicht im Curriculum der Leibniz Universität Hannover verankert sind. Diese Qualifizierungsangebote werden im Rahmen der Personalentwicklung allen Beschäftigten der Leibniz Universität Hannover angeboten.

Teilnehmende an den Kursen sind daher alle Beschäftigte, wissenschaftliche und studentische Hilfskräfte, Lehrkräfte für besondere Aufgaben, Professorinnen und Professoren, Juniorprofessorinnen und Juniorprofessoren, Promovierende ohne Beschäftigungsverhältnis, Beschäftigte von Kooperationshochschulen und in Ausnahmefällen auch externe Teilnehmende.

Ziel dieser Vereinbarung ist es, im Rahmen einer angemessenen und sinnvollen Nutzung eines Veranstaltungsmanagementsystems den Schutz der personenbezogenen Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten. Die Dienststelle und der Personalrat sind sich ferner darüber einig, dass das Veranstaltungsmanagementsystem nicht für eine Überwachung des Verhaltens und eine Arbeits- und/oder Leistungskontrolle genutzt werden darf, vielmehr ist die Gewährleistung eines Datenbestands mit transparent geregelten Zugriffsmöglichkeiten und die Vermeidung von Redundanz in der Datenhaltung Ziel des Einsatzes des Veranstaltungsmanagementsystems. Auswertungen aus dem Veranstaltungsmanagementsystem erfolgen ausschließlich innerhalb der von dieser Dienstvereinbarung und ihren Anlagen gesetzten Grenzen.

2. Gegenstand

Diese Dienstvereinbarung wird gem. §§ 59, 60, 64, 66 und 67 i.V.m. § 78 NPersVG (Niedersächsisches Personalvertretungsgesetz) geschlossen. Für die Verarbeitung personenbezogener Daten bei der Leibniz Universität gelten die Bestimmungen des Niedersächsischen Datenschutzgesetzes (NDSG) in Verbindung mit den §§ 88 ff. des Niedersächsischen Beamtengesetzes (NBG) und der Datenschutzrichtlinien der EU.

Sie definiert die Grundsätze für den Betrieb des Veranstaltungsmanagementsystems ANTRAGO

3. Geltungsbereich

Diese Dienstvereinbarung gilt für alle Beschäftigten der Leibniz Universität Hannover.

Alle Mitglieder oder Angehörigen der Hochschule, sowie alle sonstigen, nicht vom Geltungsbereich des NPersVG erfassten Personen (z.B. externe Dozierende und Teilnehmende) werden in geeigneter Form über diese Dienstvereinbarung informiert.

4. Systembeschreibung, Leistungsumfang

Das Veranstaltungsmanagementsystem ANTRAGO ist ein Datenbanksystem, in dem Daten zu Personen (Teilnehmende u. Dozierende) und Veranstaltungen erfasst und miteinander verknüpft werden können. Auf der Basis der erfassten Daten kann mithilfe der Veranstaltungsmanagementsoftware die Planung und Verwaltung erfolgen. Eine detaillierte Auflistung und Beschreibung der Veranstaltungsmanagementsoftware inkl. Systembeschreibung sowie die Details zu den zulässigen Verarbeitungen ergeben sich aus dem Fachkonzept und Datenschutzkonzept (s. Anlage 1 und 3).

Die für den Betrieb zuständige Stelle kann Änderungen, die ausschließlich dazu dienen, den technischen Betrieb sicherzustellen oder abzusichern (insbesondere Fehlerbehebung im Rahmen des sog. „Bug Fixing“ oder vergleichbare Maßnahmen) jederzeit durchführen.

5. Ziel und Zweckbestimmung des Veranstaltungsmanagementsystems

Mit dem Veranstaltungsmanagementsystem wird dem Dezernat 1 eine Unterstützung bei der Planung und Verwaltung von Qualifizierungsangeboten/-veranstaltungen und veranstaltungsbezogenen Dokumenten sowie die Ausgabe von Auswertungen zu Qualitätssicherungszwecken ermöglicht. Weitere Mandanten finden sich in Anlage 5.

Ziele sind:

- Behebung der Redundanzen in der Datenverwaltung
- Zugriff auf einen validierten und für alle Benutzerinnen und Benutzer (Sachgebiete 11 und 13) gleichen Datenbestand innerhalb eines Mandanten
- höhere Effizienz und Datenqualität bei der Planung und Verwaltung von Qualifizierungsangeboten

Details zur Nutzung und zum Einsatzzweck des Veranstaltungsmanagementsystems finden sich im Fachkonzept (s. Anlage 1).

6. Schutz der Persönlichkeitsrechte, Datenschutz und Löschkonzept

Dienststelle und Personalrat verfolgen gleichermaßen das Ziel, bei der Verarbeitung personenbezogener Daten die Persönlichkeitsrechte der Beschäftigten zu schützen. Das erfordert die eindeutige Definition von Daten, Aufgaben und Verantwortlichkeiten.

Anfallende Daten im Sinne dieser Dienstvereinbarung dürfen nur für die hier vereinbarten Zwecke verarbeitet werden. Die im Veranstaltungsmanagementsystem erfassten personenbezogenen Daten sind im Datenkatalog (Anlage 2) mit ihrer Zweckbestimmung abschließend aufgeführt und dokumentiert. Auch sofern die personenbezogenen Datenfelder mit neuen Releases der Software erweitert werden, erstreckt sich die Nutzung (z.B. für weitere Druckausgaben) ausschließlich auf die im Datenkatalog festgelegten Felder.

Die datenschutzrechtlichen Bestimmungen insbesondere der §§ 88 ff. des NBG sowie der DSGVO und des NDSG werden eingehalten. Darüber hinaus verpflichtet sich die Universität zu einem Umgang mit den persönlichen Beschäftigtendaten, der dem Grundsatz der unbedingten Erforderlichkeit der Datenerhebung, -verarbeitung und -nutzung folgt.

Das Datenschutz- und Löschkonzept inkl. einer Risikobewertung im Sinne von Art. 35 DSGVO ergeben sich aus Anlage 3 sowie der Bestätigung des Datenschutzbeauftragten, dass er Antrago nach datenschutzrechtlichen Vorgaben abgenommen und freigegeben hat (Beschreibung der Verarbeitungstätigkeit gem. Art. 30 DSGVO in Anlage 6).

7. Berechtigungskonzept

Die Zugriffsrechte der Benutzerinnen und Benutzer dienen den im Rahmen dieser Dienstvereinbarung zulässigen Aufgaben im Zusammenhang mit dem Betrieb des Veranstaltungsmanagementsystems. Das Rechte- und Rollenkonzept mit den Details zu den Berechtigungen der verschiedenen Nutzergruppen ist in Anlage 3 dargestellt.

Ein aktuelles Verzeichnis der den Rollen zugeordneten Personen kann auf Anfrage im Dezernat 1, eingesehen werden.

8. Berichte und Auswertungen

Alle veranstaltungsbezogenen Dokumente, Berichte und Auswertungen, die im Sinne dieser Vereinbarung personenbezogene Daten enthalten, sind im Reportkonzept (Anlage 4) aufgeführt und erläutert. Statistiken werden ausschließlich in anonymisierter Form erstellt.

Die Protokolldaten dienen ausschließlich den Zwecken der Gewährleistung der Systemsicherheit und der Analyse und Korrektur technischer Fehler. Der Zugriff auf die entsprechenden Programmfunktionen und die Löschrufen sind im Datenschutz- und Löschkonzept Anlage 3 erläutert.

9. Leistungs- und Verhaltenskontrolle

Die Nutzung des Veranstaltungsmanagementsystems zu weiteren Zwecken, insbesondere für Zwecke der Leistungs- und Verhaltenskontrolle oder zu Zwecken einer Ermittlung von Grundlagen für dienstliche Beurteilungen, Disziplinarmaßnahmen oder als Grundlage für die Feststellung des Gesundheitszustandes ist ausgeschlossen. Daten, die aus einer unzulässigen Nutzung stammen, dürfen nicht für arbeitsrechtliche Maßnahmen herangezogen werden. Maßnahmen, die auf Informationen beruhen,

die unter Verletzung dieser Dienstvereinbarung gewonnen werden, werden nicht durchgeführt. Wird eine missbräuchliche Nutzung festgestellt, ist die Hochschule verpflichtet, die Ursachen dafür unverzüglich abzustellen und erforderliche Maßnahmen einzuleiten.

Die Universität stellt sicher, dass die Benutzerinnen und Benutzer mit Zugang zu Reports des Veranstaltungsmanagementsystems (s. Anlage 4) auf die Einhaltung dieser Dienstvereinbarung verpflichtet werden.

10. Schnittstellen/Datenexport, -import

Ein Import personenbezogener Daten findet nicht statt.

Exporte dienen ausschließlich der weiteren Veranstaltungsabwicklung in Office sowie der Evaluation in EvaSys.

Eine Einrichtung von Schnittstellen des Veranstaltungsmanagementsystems mit anderen IT-Systemen ist vorher durch die Dienststelle mit dem Datenschutzbeauftragten und den Personalräten zu regeln.

11. Rechte der Beschäftigten, Qualifizierung

Allen Benutzerinnen und Benutzern werden erforderliche Einarbeitung, Weiterqualifizierungen und Nachqualifizierungsmaßnahmen angeboten.

Die Beschäftigten bekommen während ihrer Arbeitszeit ausreichend Zeit zur Einarbeitung und können dauerhaft auf technische Unterstützung zurückgreifen. Ihre angemessene dauerhafte informationstechnische Betreuung wird über einen persönlichen Support sichergestellt. Die Qualifizierung findet unter Fortzahlung der Bezüge und auf Kosten der Universität statt.

12. Anlagenübersicht

Anlage 1	Fachkonzept
Anlage 2	Datenkatalog <i>Die Anlage 2 zu dieser Dienstvereinbarung kann bei Herrn Dietrich im Sachgebiet 21 eingesehen werden.</i>
Anlage 3	Datenschutz- und Löschkonzept
Anlage 4	Reportkonzept
Anlage 5	Mandanten
Anlage 6	Beschreibung der Verarbeitungstätigkeit gem. Art. 30 DSGVO

13. Schlussbestimmungen, Inkrafttreten, Kündigung

Durch den Abschluss dieser Dienstvereinbarung und durch die jeweils erteilte Zustimmung des Personalrates zur Produktivsetzung des Veranstaltungsmanagementsystems gilt die Mitbestimmung gem. NPersVG - im Hinblick auf Neueinführung, Änderungen und Erweiterungen – nicht als verbraucht. Alle in dieser Dienstvereinbarung bzw. der Anlagenübersicht aufgeführten Anlagen sind Bestandteil dieser Vereinbarung.

Erweiterungen der Funktionalitäten des Veranstaltungsmanagementsystems sind vorher durch die Dienststelle mit dem Datenschutzbeauftragten und den Personalräten zu regeln

Diese Dienstvereinbarung mit Anlagen tritt am 15.08.2019 in Kraft. Sie kann einseitig unter Einhaltung einer Kündigungsfrist von 4 Monaten, frühestens jedoch zum 31.12.2020, gekündigt werden.

Sollten einzelne Bestimmungen dieser Vereinbarung insbesondere wegen Verstoßes gegen § 82 NPersVG, nichtig sein oder werden, so berührt dies nicht die Gültigkeit der übrigen Bestimmungen. Anstelle der unwirksamen Bestimmungen, oder zur Ausfüllung eventueller Lücken der Vereinbarung soll eine angemessene Regelung in Kraft treten, die dem am Nächsten kommt, was die Parteien nach ihrer Zwecksetzung gewollt haben. Im Fall der Kündigung ist das Veranstaltungsmanagementsystem

außer Betrieb zu nehmen und sämtliche Daten zu löschen. Die Dienststelle und der Personalrat verpflichten sich, im Falle der Kündigung schnellstmögliche Verhandlungen über eine Nachfolgeregelung aufzunehmen. Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform. Im Übrigen gilt § 78 Abs. 4 NPersVG.

Die Dienstvereinbarung ist allen Beschäftigten in geeigneter Weise bekannt zu machen.

Hannover, den 08.08.2019

Hannover, den 14.08.2019

Leibniz Universität Hannover
Das Präsidium

Leibniz Universität Hannover
Personalrat

gez. Prof. Dr. Volker Epping
Präsident

gez. Elli Grube
Vorsitzende

Anlage 1 Fachkonzept

Inhaltsverzeichnis

1.	Einleitung
1.5.	Ausgangssituation
1.6.	Zweck, Ziel und Vorgehensweise Fachkonzept-Entwicklung
1.7.	Verbundene Dokumente
1.8.	Abkürzungen
2.	Konzept und Rahmenbedingungen
2.1	Definition von Personenkreisen
2.2	Kernfunktionalitäten für die Benutzer
2.3.	Systemvoraussetzungen
2.4	Dokumentation/Schulung
3	Beschreibung der Anforderungen
3.1	Archivierungs- und Löschkonzept
3.2	Login/Rollen
3.3	Ressourcenverwaltung
3.4.	KIS (Kundeninformationssystem) und Wiedervorlagen
3.5.	Stammdatenverwaltung
3.6.	Qualifizierungsangebot planen und im System anlegen
3.7	Teilnehmer anmelden
3.8	Qualifizierungsangebot zusagen (Belegverfahren) und durchführen
3.9	Qualifizierungsangebot absagen (Kursausfall)
3.10	Nach Beendigung des Angebots (Abrechnung, Erfassen der Teilnahme, Teilnahmebescheinigung und Evaluation)
3.11	Reports, Listen, Abfragen
4	Schnittstellen
4.1.	Beschreibung
4.2.	Funktionalitäten
5	Import
5.1.	Beschreibungen
5.2.	Umsetzung

1. Einleitung

1.5. Ausgangssituation

Das Sachgebiet 11 – Personalentwicklung setzt im Moment drei Datenbanken auf der Basis von Access 2003 als Veranstaltungsmanagementsoftware ein. Diese Datenbanken sind eine Eigenlösung. Teilweise müssen in diesen Datenbanken Daten doppelt erfasst werden. Dies stellt eine hohe Fehlerquelle dar und führt zu mehr Zeitaufwand bei der Dateneingabe. Weiterhin sind diese Applikationen nur mit erhöhtem Aufwand auf Access 2010 (der aktuell genutzten Datenbankenanwendung in der Verwaltung der Leibniz Universität Hannover) portierbar. Zusätzlich sind fehlende Funktionen, die ausreichende Datenschutzbedingungen erfüllen, nicht vorhanden. Die Komplexität und die fehlende Dokumentation erschweren zudem den zukünftigen Support.

Im Jahr 2018 wurden mit dem jetzigen Veranstaltungsmanagement 247 Kurse mit insgesamt 291 AuftragnehmerInnen und 2.235 Teilnehmenden (3.431 Anmeldungen) in den bisherigen Datenbanken verwaltet.

Das Veranstaltungsmanagement ANTRAGO schafft die technischen Voraussetzungen für die Planung und Verwaltung von Qualifizierungsangeboten, die nicht im Curriculum der Leibniz Universität Hannover verankert sind. Diese werden im Rahmen der Personalentwicklung allen Beschäftigten der Leibniz Universität Hannover angeboten.

1.6. Zweck, Ziel und Vorgehensweise Fachkonzept-Entwicklung

Dieses Fachkonzept beschreibt die Funktionalitäten des Veranstaltungsmanagementsystems ANTRAGO der Firma RR Software GmbH. Es dient als fachliche Beschreibung des Systems, so wie es Verlauf der Implementierung auf die Bedürfnisse der Leibniz Universität Hannover (LUH) angepasst wurde.

1.7. Verbundene Dokumente

Die im Antragosystem verarbeiteten Daten sind im Datenkatalog aufgeführt. Weitere Dokumente, auf die im Fachkonzept verwiesen wird, sind das, das Datenschutz- und Löschkonzept und das Reportkonzept.

Anlage 2	Datenkatalog
Anlage 3	Datenschutz- und Löschkonzept
Anlage 4	Reportkonzept
Anlage 5	Mandanten

1.8. Abkürzungen

VM = Veranstaltungsmanagement
 TN = Teilnehmer
 PE = Sachgebiet 11 - Personalentwicklung
 Reports = Bezeichnet die Ansicht und/oder den Ausdruck von Listen und Übersichten in unterschiedlichen Funktionen und Prozessen.

2 Konzept und Rahmenbedingungen

2.1 Definition von Personenkreisen

Im Konzept wird es unter folgenden Personenkreisen unterschieden: BenutzerInnen, Teilnehmende und AuftragnehmerInnen, die wie folgt definiert und beschrieben werden:

BenutzerInnen sind Beschäftigte, die für planerisch/administrativen Prozesse im Veranstaltungsmanagement zuständig sind und die Software zur Unterstützung dieser Prozesse aktiv nutzen. Der Benutzerkreis beschränkt sich auf ca. 18 Beschäftigte, die das Qualifizierungsangebot im Dezernat 1 – Organisations- und Personalentwicklung und IuK-Technik betreuen. Hierfür sind Concurrent Lizenzen im Einsatz.

Teilnehmende der Qualifizierungsangebote sind Beschäftigte der Leibniz Universität Hannover, Lehrkräfte für besondere Aufgaben, ProfessorInnen, JuniorprofessorInnen, Tenure Track ProfessorInnen, Promovierende ohne Beschäftigungsverhältnis, Beschäftigte von Kooperationseinrichtungen und in Ausnahmefällen auch externe Teilnehmende. Sie haben keinen Benutzerzugriff auf Antrago.

AuftragnehmerInnen sind DozentInnen, Coaches und BeraterInnen, die mit der Durchführung der Qualifizierungsangebote beauftragt werden. Sie haben keinen Benutzerzugriff auf die Software.

2.2 Kernfunktionalitäten

- Verwaltung der Veranstaltungsdaten der Qualifizierungsangebote: Dokumentation und Management des gesamten Prozesses von der Planung, über die Abwicklung bis zur Auswertung der Qualifizierungsangebote, inkl. Erstellung erforderlicher Reports und Listen
- Datenverwaltung von Teilnehmenden: Stammdatenverwaltung, Dokumentation und Management von Anmeldungen, Teilnahmen etc., Erstellung erforderlicher Reports
- Datenverwaltung von AuftragnehmerInnen (DozentInnen, Coaches, BeraterInnen): Stammdatenverwaltung, Dokumentation und Management von Aufträgen, Erstellung erforderlicher Reports
- Verwaltung bzw. Buchung von Ressourcen (Räume, technische Ausstattung etc.)
- Erstellung von Statistiken
- Budgetplanung bzw. -verwaltung (DozentInnenhonorare, Fahrtkosten, Umsatzsteuer)
- Querschnittsfunktionen wie Workflowmanagement und Dokumentenmanagement

Die Applikation ist optional auf ergänzende Web-Funktionen (Online-Anmeldung, Bestätigung, etc.) erweiterbar.

Die Software ist mandantenfähig. Eine Nutzung des Antragosystems durch weitere AkteurInnen der Personalentwicklung (als weitere MandantInnen) wird angestrebt und unter Berücksichtigung der Dienstvereinbarung realisiert. (siehe Anlage 5)

2.3 Systemvoraussetzungen

Systembeschreibung siehe Datenschutz- und Löschkonzept (Anlage 3)

2.4 Dokumentation/Schulung

Eine Dokumentation in gedruckter Form oder als PDF-Datei steht den BenutzerInnen zur Verfügung. Zusätzlich erhalten sie eine Anwenderschulung.

3 Beschreibung der Anforderungen

3.1 Archivierungs- und Löschkonzept

Siehe Anlage 3

3.2 Login/Rollen

Das Arbeiten mit der VM-Software ist nur mit autorisiertem Login möglich. Hierzu können Rechte auf diverse AnwenderInnengruppen bis auf Feldebene vergeben werden. Bei Zuordnung mehrerer Gruppenrechte verhalten sich die Rechte kumulativ.

Einzelheiten zum Rechte-/Rollenkonzept siehe Anlage 3

3.3 Ressourcenverwaltung

3.3.1. Beschreibung

- Die zentrale Raumbuchung und -vergabe der Universität erfolgt durch das System LSF, künftig SAP, auch die Räume der PE werden dort verwaltet. Während des Planungszeitraums für das Weiterbildungsprogramm übernimmt das VM-System eine koordinierende Funktion (verhindert Doppelbuchungen). Sobald der Planungszeitraum abgeschlossen ist, werden die Buchungen in das führende System (LSF) übertragen.
- Raumbuchung erfordert eine hohe Flexibilität: es gibt Veranstaltungen, die mehrere Räume pro Tag zu unterschiedlichen Uhrzeiten erfordern, oder für jeden einzelnen Termin einen unterschiedlichen Raum. Dies ist abbildbar.
- Bei Kurszusagen für Teilnehmende und AuftragnehmerInnen werden alle Termine mit dem jeweiligen Raum aufgeführt. (Bei Veranstaltungsreihen bezogen auf die gesamte Reihe)
- Weitere Ressourcen (Ausstattungsmerkmale, Geräte, Software) werden im VM-System einzeln zur Veranstaltung hinzugebucht.

3.3.2. Funktionalitäten bei der Ressourcenverwaltung

- Anlage, Belegung/Buchung und Verwaltung von Ressourcen, incl. Informationen zu Rahmen- daten wie Raumgröße, Plätze, Raumausstattung, Raumverantwortliche etc.
- Zuordnung von Dateien pro Ressource (z. B. Hinweisschilder, Nutzungsinfos, Lagepläne) möglich
- Verhinderung Doppelbelegung durch Plausibilitätsprüfung
- Im Kalender werden übersichtlich die gebuchten Kurse pro Raum und die gebuchten Geräte angezeigt.
- Kalenderfunktion mit Darstellung freier und gebuchter Zeiträume sowie Feiertage/Schulferien in Niedersachsen, Wochenenden, vorlesungsfreier Zeiträume.
- Darstellung von Erstbuchungs- bzw. Vorbelegungsrechten
- Vergabe eines Buchungsstatus pro Termin, bspw. vorbehaltliche Buchung, feste Buchung, angefragte Reservierung anderer Einrichtungen

3.4. (Kundeninformationssystem) KIS und Wiedervorlagen

3.4.1. Beschreibung

Im Kunden Informationssystem (KIS) werden Kommunikationsvorgänge innerhalb des BenutzerInnenkreises sowie mit Teilnehmenden, AuftragnehmerInnen und Firmen dokumentiert.

Im KIS werden die Kommunikationsvorgänge gegliedert nach Vorgangsarten, die sich aus dem Prozess der Planung und Abwicklung der Qualifizierungsangebote ergeben, dargestellt.

Die Versendung von Anschreiben und anderen Reports, für Teilnehmende, AuftragnehmerInnen und Firmen wird unter Berücksichtigung der Vorgangsart im KIS-System automatisch vermerkt. Das versendete Dokument kann wahlweise mit gespeichert werden. KIS-Einträge können entweder bei der Veranstaltung oder bei der Person dokumentiert werden

Wiedervorlagen können an die eigene Person oder an andere BenutzerInnen oder eine Abteilung gerichtet werden. Das Dezernat 1 hat zwei Abteilungen gebildet, die sich auf die Aufgaben beziehen: ProgrammverwalterInnen und ProgrammplanerInnen (siehe 3.6.1). So können Wiedervorlagen an eine Gruppe von Personen mit gleicher Aufgabe gestellt werden. Wiedervorlagen können sich auf Veranstaltungen, AuftragnehmerInnen, Teilnehmende und Firmen beziehen.

Ein KIS-Eintrag kann mit einer Wiedervorlage verknüpft werden, um die Weiterbearbeitung sicherzustellen.

Eine detaillierte Darstellung der im KIS und in den Wiedervorlagen verarbeiteten Daten, siehe Anlage 2

3.4.2. Funktionalitäten

- Erstellen von KIS-Einträgen und Wiedervorlagen aus Personen-, Firmen- und Veranstaltungsfenstern
- Automatische Erstellung von KIS-Einträgen bei der Generierung von Reports
- Anzeigen aller von dem/der BenutzerIn gestellten sowie an den/die BenutzerIn gestellten Wiedervorlagen in einer persönlichen Liste mit Filtermöglichkeit (Druckfunktion)

- Darstellung der KIS-Einträge in Personen-, Veranstaltungs- und Firmenfenstern (kann gefiltert/sortiert werden)
- Anzeige einer Liste von KIS-Einträgen mit Filtermöglichkeit

3.5. Stammdatenverwaltung

Für alle in der Software erfassten Personen werden grundlegende Stammdaten (Anrede, Titel, Vorname, Nachname) erfasst. Dabei kann jede Person in beliebigen Kombinationen Personenkreisen (BenutzerIn, TeilnehmendeR, AuftragnehmerIn) zugeordnet werden. Es kann vorkommen, dass eine Person zu allen Personenkreisen zugeordnet ist. Die Personendaten werden so erfasst, dass dabei keine Dubletten entstehen.

3.5.1. BenutzerInnen

siehe Datenkatalog (Anlage 2)

3.5.2. Teilnehmende

Siehe VM_DV_Datenkatalog_Antrago.docx

3.5.3. AuftragnehmerInnen (Dozenten/Coaches/Berater)

siehe Datenkatalog (Anlage 2)

3.5.4. Firmen

siehe Datenkatalog (Anlage 2)

3.6. Qualifizierungsangebot planen und im System anlegen

3.6.1. Beschreibung der Angebotsstruktur

Die Qualifizierungsangebote des Sachgebiets Personalentwicklung werden in unterschiedlichen didaktischen Formaten angeboten (bspw. Kurse, Coaching, Mentoring etc.), die sich im VM-System hinsichtlich ihrer Merkmale wie der zeitlichen Gestaltung, Anzahl der Teilnehmenden, der Binnenstruktur (Anzahl von assoziierten Veranstaltungen) differenziert darstellen lassen. Es ist möglich, weitere Eigenschaften der Qualifizierungsangebote zu erfassen, wie Teilnahmevoraussetzung und Zielgruppendefinition und im Verlauf der Qualifizierungsabwicklung bspw. bei der Teilnehmendenzusage zu berücksichtigen.

Qualifizierungsangebote können aus einem Einzeltermin oder mehreren Terminen bestehen, tw. in Kombination mit Einzelcoaching-Elementen. Die Uhrzeiten und Orte können zwischen den Terminen variieren.

Das Sachgebiet Personalentwicklung bietet „Veranstaltungsreihen“, bestehend aus mehreren Kursen (Module genannt), an. Diese lassen sich entsprechend im System abbilden. Teilnehmende werden bei der Anmeldung für die gesamte Reihe und zusätzlich für Wahlpflichtveranstaltungen individuell registriert. Eine Mindestteilnehmendenzahl, die sich auf die gesamte Veranstaltungsreihe bezieht, wird kontrolliert.

Im Antrago-System können die Qualifizierungsangebote unterschiedlichen Veranstaltungsarten zugeordnet werden. Das Sachgebiet Personalentwicklung nutzt diese Funktionalität, um unterschiedliche Qualifizierungsangebote (bspw. Weiterbildungsprogramm) bzw. „thematische Qualifizierungsbereiche“ (bspw. Personalentwicklung für die Lehre, Personalentwicklung für Führungskräfte etc.) strukturell voneinander abzugrenzen. Die Veranstaltungsarten lassen sich ergänzen und umstrukturieren. Innerhalb der Veranstaltungsarten erfolgt eine weitere Untergliederung, die pro Veranstaltungsart definiert werden kann.

Manche Qualifizierungsangebote sind einer Veranstaltungsart zugeordnet, sind darüber hinaus aber auch für einen anderen Bereich relevant (bspw. als Wahlpflichtveranstaltung). Dies kann bei den Veranstaltungen erfasst, im Verlauf der Qualifizierungsabwicklung über flexible Listen angezeigt und bspw. in Zertifikaten berücksichtigt werden.

Den Qualifizierungsangeboten kann in Antrago ein Stab zugeordnet werden. Das Sachgebiet Personalentwicklung nutzt dies, um interne Zuständigkeiten nachvollziehbar zu machen. Personen, die konzeptionell, planerisch für die Veranstaltung verantwortlich sind, werden als „ProgrammplanerIn“, Personen, die für die organisatorische Abwicklung zuständig sind, als „ProgrammverwalterIn“ zugeordnet. Die Qualifizierungsangebote erhalten für organisatorische Zwecke einen Status, der den Bearbeitungsstand kennzeichnet. Folgende Status können im Verlauf der Planung und Abwicklung eines Angebots vergeben werden:

- Planung vorbehaltlich
- Planung
- Planung abgeschlossen
- Anmeldung
- Durchführung (zugesagt)
- Storno (abgesagt)
- abgerechnet

3.6.2. Funktionalitäten

- Stammdaten des Qualifizierungsangebots erfassen, ändern und löschen :
 - Kurs-Nr., Kurstitel, Ausschreibungstext, Termine (semesterunabhängig), Anmeldeschluss, Ressourcen, Kostenstelle/Projektnummer, Sachkonto, Zielgruppe, Teilnahmevoraussetzung, Zusatztexte, Auftragnehmer (Dozenten/Coaches/Berater), Raumvorbereitungen, Teilnehmer Mind./Max.,
 - Kursinhalt, der auf die Teilnahmebescheinigung aufgedruckt wird
 - Hinzufügen von Anlagen pro Angebot in Word, Excel und PDF (z. B. Kursunterlagen von AuftragnehmerInnen, Buchungsbestätigung des Hotels)
 - Kennzeichnung von Terminen als Coaching-Termine (Einzelcoaching innerhalb des Kurses)
 - Erfassen von KooperationspartnerInnen (z. B. MHH, FHH, VHS), (ggf. Berücksichtigung bei der Reihung der Teilnehmenden bei Kurszusage)
 - Kurs nur für Beschäftigte (intern) Ja/Nein
 - Raumvorbereitung: Bestuhlung, Tischform, technische Ausstattung, Ankunftszeit AuftragnehmerIn vor Ort etc.)
 - Informationen zur Kursorganisation (z. B. Hinweise zum Stand der Planung/Sachbearbeitung)
 - Finanzen: Kursgebühren erfassen und ausweisen; Preisstaffelung nach Teilnehmendengruppen (änderbar); Preisgruppe 1: interne Teilnehmende (immer 0,00 €); Preisgruppe 2: externe Teilnehmende
- Qualifizierungsangebote können einzeln oder in Massenkopie (einschränkbar) aus vorherigen Zeiträumen kopiert werden
- Berechnung der geplanten Kosten (SOLL) und der tatsächlichen Ausgaben (IST) pro AuftragnehmerIn und pro Qualifizierungsangebot anhand der eingegebenen Daten (Gesamthonorar des Dozenten + Reisekosten + Hotelkosten)
- Abgleich der geplanten Kosten und der Ausgaben mit einem hinterlegten Budget

3.6.3. Zusätzliche Funktionalitäten für offene Veranstaltungen ohne Teilnehmerliste

- Erfassen der Teilnehmendenzahl (ohne Erfassung der Teilnehmerdaten) (für statistische Auswertung)

3.6.4. Zusätzliche Funktionalitäten für Externe Weiterbildung

- Kursstammdaten von externen WeiterbildungsanbieterInnen erfassen, ändern und löschen
- Vergabe von individuellen Kursnummern mit unterschiedlicher Formatierung (z. B. 14-01-000, 16.01.132, 45, ...) Möglichkeit, Kurse anhand der eingegebenen Kursnummer zu sortieren. Möglichkeit, innerhalb des Produktes zwischen den Kursen zu navigieren, ohne das andere Kurse aus anderen Produktbereichen dazwischenkommen.

- Erfassen des AnbieterInnennamens, des AnbieterInnenkürzels sowie der Adresse des/der Anbieters/Anbieterin
- geplante Kosten pro Kurs und pro teilnehmender Person hinterlegbar
- Kennzeichnung von gebührenfreien Kursen

3.7 Teilnehmer anmelden

3.7.1. Beschreibung

Bei dem Anmeldeprozess werden die Anmeldungen im System durch die BenutzerInnen registriert. Es werden jedoch zunächst noch keine Teilnehmendenplätze vergeben. Dies geschieht erst zum Zeitpunkt der Zusage des Qualifizierungsangebots (siehe 3.8). Dann werden die Teilnehmenden nach diversen Kriterien gereiht (Abgleich Zielgruppe, Abgleich Teilnahmevoraussetzung, Teilnehmerkategorie (ext./int...), Anmeldezeitpunkt) und zugesagt, bzw. bei Überbelegung teilweise abgesagt. Diese Kriterien werden im System abgebildet, und bereits bei der Anmeldung erfasst. Zusätzlich kann bei der Anmeldung eine Priorität in Form eines Zahlencodes vergeben werden, der das Ranking der Teilnehmenden bei Überbelegung ebenfalls beeinflusst. Je nach Qualifizierungsangebot variieren die zu berücksichtigenden Kriterien bei der Reihung der Teilnehmenden und können entsprechend berücksichtigt werden.

Interne Teilnehmende werden bevorzugt behandelt und können kostenlos an den Qualifizierungsangeboten teilnehmen. Bei manchen Angeboten dürfen keine externen Personen teilnehmen. Teilnehmende von Kooperationshochschulen können an Kooperationsangeboten teilnehmen und werden gleichwertig wie interne Teilnehmende behandelt. Wenn Beschäftigte von Kooperationshochschulen sich zu Qualifizierungen anmelden, für die keine Kooperation verabredet wurde, werden sie wie externe Teilnehmende behandelt. Die externen Teilnehmenden werden bei der Belegung der Qualifizierungsangebote nachrangig behandelt.

Teilnehmende erhalten für organisatorische Zwecke einen Status. Folgende Status sind möglich:

- InteressentIn
- Teilnahme
- Rücktritt

Das Anmeldedatum sowie das Datum der Kurszusage, -absage, Nachrückdatum, Rücktrittsdatum werden automatisch erfasst. Übersichtliche Darstellung der Historie einer Person (Anmeldungen/bereits teilgenommene Kurse/Rücktritte)

3.7.2. Funktionalitäten

- Übersichtliche und unkomplizierte Erfassung der Anmeldungen durch die BenutzerInnen im System:
 - Erfassen, ob Teilnahmevoraussetzungen erfüllt sind (z. B. Besuch Grundkurs)
 - Erfassen der Zustimmung der/des Vorgesetzten (Unterschrift auf Teilnahmeantrag)
- Anmeldungen: Die Summe der Anmeldungen wird im Feld „Interessent“ angezeigt
- Bei Veranstaltungsreihen und beim Mentoring: Teilnehmende werden bei der Anmeldung wahlweise für alle Module der Veranstaltungsreihe bzw. des Mentorings registriert oder für Wahlpflichtveranstaltungen individuell. Ggf. wird bei Wahlpflichtveranstaltungen erfasst dass die „Veranstaltung wird auf Zertifikat XY“ angerechnet wird.
- perspektivisch ist eine Online-Anmeldung möglich
- Anmeldebestätigung per E-Mail (kann optional gesendet werden) (bei Veranstaltungsreihen bezogen auf das gesamte Programm)
- Erfassen von Rücktritten (bei Veranstaltungsreihen pro Modul)
- Erfassen von Kriterien, die die Teilnehmendenreihung bei einer Überbelegung des Qualifizierungsangebots beeinflussen (bspw. Zielgruppenzugehörigkeit, dienstliche Dringlichkeit, bereits erfolgte Ablehnung aufgrund von Überbelegung oder aus dienstlichen Gründen etc.)

3.7.3. Besondere Funktionalitäten für externe Weiterbildung

- Kennzeichnung der eingegebenen Anmeldung mit einem Merkmal (Kosten werden übernommen/nicht übernommen)
- Erfassung der Tätigkeit der/des Teilnehmenden
- Anmeldung wurde wie vorgenommen? (Online, per Fax, per Brief etc.)

- Erfassen des Eingangsdatums sowie des Anmeldedatums

3.8 Qualifizierungsangebot zusagen (Belegverfahren) und durchführen

3.8.1. Beschreibung

Sobald der Anmeldeschluss erreicht ist, listet das System das Qualifizierungsangebot in einer Abfrage auf und weist somit die zuständigen KursverwalterInnen darauf hin.

Beim Weiterbildungsprogramm ist es in einem ersten Schritt erforderlich die Teilnehmenden zu reihen. Unter Berücksichtigung diverser Kriterien (siehe 4.7.1) schlägt das System eine Reihung der Teilnehmenden vor, die von den KursverwalterInnen ausgedrückt werden kann. Die Reihung kann verändert werden. Danach kann eine Entscheidung erfolgen, wer eine Zu-/Absage erhält. Das System erstellt entsprechend der Entscheidung die Reports für die Kurszu- und -absagen. Die erstellte Liste der gereihten Teilnehmenden kann anschließend mit einem Anschreiben für den Personalrat ausgedruckt werden.

Eine Zusage mit Rechnungsstellung ist optional möglich.

Unterlagen für AuftragneherInnen werden vor der Durchführung des Qualifizierungsangebotes vom System erstellt. Dazu gehören Teilnehmendenliste und Teilnahmebescheinigungen.

Am Veranstaltungstag werden die meisten Veranstaltungen mit Beschäftigten der PE vor Ort betreut. Hierfür wird der Raumvorbereitungszettel benötigt. Zur internen Koordination, wer sich um welche Veranstaltung kümmert, werden Veranstaltungslisten mit Datum, Uhrzeit und Raum benötigt.

3.8.2.Funktionalitäten

- Mittels einer Abfrage im System wird den ProgrammverwalterInnen angezeigt, bei welchen Qualifizierungsangeboten der Anmeldeschluss abgelaufen und somit eine Zu-/Absage erforderlich ist. Nach der Kursbestätigung wird der entsprechende Kurs nicht mehr in der Abfrage angezeigt. In einer weiteren Abfrage werden alle zugesagten Kurse bei denen der Kursbeginn in 4 Tagen bzw. in 1 Tag sein wird, dargestellt.
 - Die KursverwalterInnen haben die Möglichkeit, auszuwählen welche/r SachgebietsleiterIn/Vertretungskraft bzw. welche KursplanerInnen auf den entsprechenden Dokumenten (bspw. Kopfbogen bzw. Teilnahmebescheinigung) angezeigt werden sollen.
 - Erfassung von Zusatztexten für die Kurszusagen an die Teilnehmenden und AuftragnehmerInnen (Anzeige in Mail und Anschreiben)
 - Überprüfung durch das System: Liegt die (schriftliche) Stellungnahme der/des Vorgesetzten vor? (Ja/Nein)
Wenn nein wird in die Kurszusage ein Hinweis aufgenommen, dass die Stellungnahme der/des Vorgesetzten nachgereicht werden muss
- Erinnerungsfunktionen durch Wiedervorlagen und das interne Kommunikationssystem KIS
- Warteliste: Sobald ein Angebot zugesagt ist, wird bei Überbelegung die Summe der Personen, die keinen Platz erhalten hat im Feld „Interessent“ angezeigt
- Reihung der Teilnehmenden bei Überbelegung eines Qualifizierungsangebots: Reihung der angemeldeten Personen nach den erforderlichen Kriterien (bspw. Zielgruppe, Abgleich Teilnahmevoraussetzung, Teilnehmendenkategorie (ext./int...), Berücksichtigung bereits erfolgter Ablehnung aufgrund von Überbelegung oder aus dienstlichen Gründen, Anmeldedatum). Die Reihung der Teilnehmenden kann verändert werden.

3.8.3. Zusätzliche Funktionalitäten für Veranstaltungsreihen mit mehreren Modulen

- Zusage und Absage bezieht sich auf die gesamte Veranstaltungsreihe inkl. Informationen zu allen Modulen
- Erinnerungs-E-Mail an alle Teilnehmenden eine Woche vor jedem Modul mit allen Informationen.
- Rücktritt für einzelne Teile der Veranstaltungsreihen möglich

3.8.4. Zusätzliche Funktionalitäten für Mentoring

- Zusage und Absage bezieht sich auf das gesamte Mentoring-Programm, differenziert nach Mentor/Mentee
- Rücktritt für einzelne Teile des Mentorings ist möglich

3.8.5. Zusätzliche Funktionalitäten für Externe Weiterbildung

- Erfassen des Status (Kurs noch nicht bestätigt, Kurs zugesagt) pro Kurs (händisch)
- Erfassen des Status (Kurs noch nicht bestätigt, Teilnahme zugesagt, Rücktritt) der Teilnehmenden (händisch)
- Erfassung des Zusagedatums, des Rechnungsdatums bzw. des Bezahldatums
- Kosten pro Person hinterlegbar

3.9 Qualifizierungsangebot absagen (Storno/Kursausfall)**3.9.1. Beschreibung**

Wird die Mindestteilnehmerzahl des Qualifizierungsangebotes unterschritten, so wird das Angebot abgesagt. Die Entscheidung darüber liegt bei den KursplanerInnen, wird von den KursverwalterInnen im System umgesetzt und wird nicht automatisch vom System ausgeführt. Das System erstellt bei der Entscheidung für eine Absage die betreffenden Dokumente für AuftragnehmerInnen und die angemeldeten Personen.

3.9.2. Funktionalitäten

- Möglichkeit, Zusatztexte zu hinterlegen, die auf den Kursabsagen an die Teilnehmenden bzw. an die AuftragnehmerInnen angezeigt werden
- Datum des Qualifizierungsangebotsausfalls automatisch erfassen
- bei Ausfall des Qualifizierungsangebots werden die geplanten Termine automatisch aus dem Kalender gelöscht
- Absage des Qualifizierungsangebots ist auch möglich, nachdem das Angebot bereits zugesagt wurde (z. B. kurzfristige Erkrankung der AuftragnehmerInnen)

3.9.3. Zusätzliche Funktionalitäten für Veranstaltungsreihen mit mehreren Modulen

- Absage bezieht sich auf die gesamte Veranstaltungsreihe.

3.9.4. Zusätzliche Funktionalitäten für Externe Weiterbildung

- Erfassen des Status (Teilnahme abgelehnt, Kurs ausgefallen) der Teilnehmenden (händisch)
- Erfassung des Absagedatums

3.10. Nach Beendigung des Angebots (Abrechnung, Erfassen der Teilnahme, Teilnahmebescheinigung und Evaluation)**3.10.1. Beschreibung**

Nach der Veranstaltung erfolgt die Abrechnung des Angebots durch die AuftragnehmerInnen. Hier ist es wichtig, die abgerechneten Summen zu erfassen, um einen Abgleich von Plan und Ist zu ermöglichen.

Die Angebote der PE werden in Papierform evaluiert. Der Evaluationsbogen wird außerhalb des VM-Systems mit EvaSys erstellt. Die Bögen werden mit EvaSys ausgewertet. Die Evaluationsergebnisse werden den AuftragnehmerInnen per Mail zugeschickt.

Beim Coaching werden die Bögen nach einem festgelegten Zeitraum an die Teilnehmenden verschickt.

Bei allen Qualifizierungsangeboten wird nach Abschluss die Teilnahme erfasst und im System dokumentiert.

3.10.2. Funktionalitäten

- Unterstützung bei der Abrechnung der Qualifizierungsangebote: Dokumentation „Veranstaltung ist abgerechnet“, Erfassen der abgerechneten Beträge (Honorar, Reisekosten, Hotelkosten)
- Erfassung der Abwesenheiten (tage- und stundengenau). Teilnehmende gelten als anwesend, wenn keine Abwesenheit erfasst wurde. So kann bspw. berechnet werden, ob Voraussetzungen für ein Zertifikat erfüllt sind.

3.10.3. Zusätzliche Funktionalitäten für Mentoring und Coaching:

- Im System werden die Leistungen erfasst (Teilnahme an Veranstaltungen/Durchführung kollektiver Hospitation oder Teilnahme an X Coaching-Stunden)
- Teilnahmebescheinigungen enthalten nur absolvierte Leistungen des Programms
- Erinnerung an die Versendung des Evaluationsbogens über eine Wiedervorlage

3.10.4. Zusätzliche Funktionalitäten für Veranstaltungsreihen mit mehreren Modulen:

- Teilnahmebescheinigung pro Modul
- Es werden Zertifikate erstellt, die alle Elemente der Veranstaltungsreihe, inkl. der Wahlpflichtveranstaltungen (die pro TN variieren) enthalten.
- Das System überprüft, ob die Mindestanwesenheitspflicht bezogen auf die gesamte Veranstaltungsreihe inkl. Modul gegeben ist und stellt nur dann ein Zertifikat aus.

3.11 Reports, Listen, Abfragen

Siehe Anlage VM_ReportsListenAbfragen.docx

4 Schnittstellen**4.1. Beschreibung**

Exporte dienen ausschließlich der weiteren Veranstaltungsabwicklung in Office sowie der Evaluation in EvaSys.

4.2.Funktionalitäten

- Erstellen von Serienbriefen z. B. in MS Word für die Kurszu- und -absagen, Teilnahmebescheinigungen o. ä.
- Das Versenden von E-Mails an Teilnehmende und AuftragnehmerInnen ist über die Anbindung an MS Outlook auch mit Platzhaltern und Textbausteinen gegeben
- Erstellen von Auswertungen z. B. in MS Excel (Bspw. Finanzdaten)

5 Import

Es erfolgt kein Import personenbezogener Daten aus anderen Systemen in Antrago. Es werden Einrichtungsdaten der LUH aus LSF in Antrago eingelesen (Kostenstellen, Fakultäten/Dezernate/Einrichtungen, Institute/Sachgebiete)

Anlage 3 Datenschutz- und Löschkonzept

Inhalt

1. Präambel, Einleitung
 - 1.1 Mitgeltende Unterlagen
2. Systembeschreibung, technische Maßnahmen/ Daten, Sicherung
 - 2.1 Veranstaltungsmanagementsystem ANTRAGO
 - 2.2 Schutzbedarf
 - 2.3 Schutzstufe aus Datenschutz-Sicht
 - 2.4 Schutzbedarf aus Sicht der Informationssicherheit
3. Hosting IuK
 - 3.1 Hardware
 - 3.2 Netzwerk
 - 3.3 Software
4. Technisch-organisatorische Maßnahmen des Datenschutzes
 - 4.1 Zugangskontrolle
 - 4.2 Datenträgerkontrolle
 - 4.3 Speicherkontrolle
 - 4.4 Benutzerkontrolle
 - 4.5 Zugriffskontrolle
 - 4.6 Übermittlungskontrolle
 - 4.7 Notfallplan
5. Datenkategorien
 - 5.1 Personenkreise
 - 5.2 Datenkatalog
 - 5.3 Datenverarbeitung
 - 5.4 Datenarten und Zwecke der Datenverwendung
 - 5.5 Rechtsgrundlage für Datenspeicherung/-verarbeitung
6. Zugriffsregelungen/Aufgaben/Rollen und Rechte
 - 6.1 Nutzergruppen
 - 6.2 Rollen und Rechte auf Datenbankebene
 - 6.3 Rollen und Rechte auf Anwendungsebene
 - 6.3.1 Rechte für Rolle PraktikantIn
 - 6.3.2 Rechte für die Rolle Studentische Hilfskraft:
 - 6.3.3 Rechte für ProgrammplanerInnen:
 - 6.3.4 Rechte für die Rolle Vorgesetzte
7. Lösch- und Anonymisierungskonzept
 - 7.1 Fristen für Löschung und Anonymisierung
 - 7.2 Umsetzung der Anonymisierung und Löschung
 - 7.2.1 Vorgehensweise der statistischen Auswertung
 - 7.2.2 Vorgehensweise der Datenlöschung
8. Risikoanalyse
 - 8.1 Gefahren- und Risikoanalyse

1. Präambel, Einleitung

1.1 Mitgeltende Unterlagen

- Meldung zum Verzeichnis der Verarbeitungstätigkeiten
- Datenkatalog
- Reportkatalog

2. Systembeschreibung, technische Maßnahmen/ Daten, Sicherung

Das Veranstaltungsmanagement ANTRAGO schafft die technischen Voraussetzungen für die Planung und Verwaltung von Veranstaltungen, die nicht im Curriculum der Leibniz Universität Hannover verankert sind. Diese Qualifizierungsangebote werden im Rahmen der Personalentwicklung allen Beschäftigten der Leibniz Universität Hannover angeboten.

Aus dem Altsystem werden keine personenbezogenen Daten in das das Veranstaltungsmanagementsystem ANTRAGO übernommen.

Das Veranstaltungsmanagement ANTRAGO der Fa. RR Software GmbH wird auf einem Server im Netz der Verwaltung durch das Dezernat 1, SG 12 (IuK) bereitgestellt. Die IuK betreibt den notwendigen Server, sorgt für das Backup der Daten und administriert die technische Seite der Applikation.

2.1 Veranstaltungsmanagementsystem ANTRAGO

Das Veranstaltungsmanagementsystem ANTRAGO der Firma RR Software GmbH ist ein ausführbares Programm. Die Anwendung läuft zentral auf dem Antrago Server (uhv-antrago) im Verwaltungnetz. Während der Nutzung der Anwendung greifen alle berechtigten BenutzerInnen über eine Verknüpfung auf dieses Programm zu. Es bedarf daher keiner weiteren Software Installation am Client-PCs.

Die Applikation greift auf dem Fileserver in einem nur von berechtigten BenutzerInnen zu nutzenden Verzeichnis auf gespeicherte Dateien (Reportvorlagen) und auf dem Applikationsserver (uhv-antrago) auf in einer relationalen Datenbank abgelegte Daten zu.

Die Kernanwendung des Veranstaltungsmanagementsystems ANTRAGO dient der Dateneingabe von Stamm- (BenutzerInnen, Teilnehmenden, DozentInnen) und Veranstaltungsdaten und den Verknüpfungen zwischen Veranstaltungen, Teilnehmenden und DozentInnen. Darüber hinaus ermöglicht die Applikation die Erstellung der für den Anwendungszweck notwendigen Korrespondenz.

Sie wird ausschließlich nach einem Login durch benannte Benutzer verwendet, die grundsätzlich Angehörige der LUH sind.

2.2 Schutzbedarf

Grundsätzlich muss im Fachkonzept der Schutzbedarf festgestellt werden. Darüber hinaus wird hier noch einmal eine Risikobetrachtung durchgeführt, um die Maßnahmen für das Hosting abzuleiten. Falls der Schutzbedarf im Fachkonzept als höher angesehen wird, muss geklärt werden, ob die Sicherheitsmaßnahmen dennoch ausreichend sind.

2.3 Schutzstufe aus Datenschutz-Sicht

Die Schutzbedarfsfeststellung für die personenbezogenen Daten erfolgt anhand des Schutzstufenkonzepts der Landesbeauftragten für den Datenschutz Niedersachsen⁴.

Zu den BenutzerInnen werden im System Nutzernamen und Passwörter hinterlegt.

Schutzstufe: B

Das Veranstaltungsmanagementsystem ANTRAGO wird mit im Wesentlichen mit Daten von Organisationseinheiten und Personen (interne Teilnehmende und DozentInnen) der Leibniz Universität befüllt. Diese sind zumindest innerhalb der Leibniz Universität alle öffentlich, entsprechen den Eintragungen befinden sich in Personen & Einrichtungsverzeichnissen.

Schutzstufe: B

Bei externen Personen (DozentInnen) ist die Einverständniserklärung notwendig.

Nicht die Einzeldaten, aber die Verknüpfungen zwischen Veranstaltungen und einer Person sind anders einzuordnen.

Schutzstufe: C

Insgesamt ist höchstens von *Schutzstufe C* auszugehen: „Personenbezogene Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte (Ansehen).“

2.4 Schutzbedarf aus Sicht der Informationssicherheit

Die Schutzbedarfsfeststellung erfolgt angelehnt an die Vorgehensweise des IT-Sicherheitskonzepts der ZUV⁵

Insbesondere werden die dort definierten nichtquantifizierten Schadenskategorien übernommen.

Verfügbarkeit: normal

Durch einen temporären Ausfall des Datenbankmanagementsystems können Arbeitsabläufe erheblich behindert und verzögert werden. Image-Schäden sind möglich. Der generelle Betrieb der Universität ist jedoch nicht gefährdet.

Die Zentralinstallation und die Datenbankapplikation (MSSQL) laufen als virtuelles System. Die Verfügbarkeit ist hauptsächlich durch technische Defekte gefährdet. Diese werden durch die Auswahl geeigneter hochwertiger Hardware und dem Betrieb in einem zentralen Technikraum mit hochverfügbaren Versorgungssystemen minimiert. Zusätzlich wird das virtuelle System auf eine weitere Virtualisierungsplattform repliziert, um im Fehlerfall dort den Betrieb kurzfristig mit der Replik fortsetzen zu können. Zusätzlich werden die Systeme regelmäßig gesichert. Obwohl kein redundantes System zur Verfügung steht, kann das System auf diese Weise im Fehlerfall zeitnah weiterbetrieben werden. Es ist daher nur von einer geringen technischen Gefährdung der Verfügbarkeit auszugehen.

Unbeabsichtigte Fehlkonfigurationen werden durch eine geeignete Einarbeitung der administrativ tätigen Verantwortlichen soweit möglich vermieden.

Eine Überlastung oder Störung des Systems durch unsachgemäßen Betrieb, ist softwareseitig schwer möglich. Für reguläre Anfragen wurde das System im Vorfeld ausreichend dimensioniert.

Eine mutwillige Gefährdung der Verfügbarkeit durch Sabotage, Manipulation und Diebstahl wird durch eine protokollierte Zugangskontrolle und eingeschränkte administrative Zugänge erheblich minimiert. Aufgrund der dezentralen Bedeutung des Service und der damit verbundenen geringen Attraktivität für potentielle Angreifer kann das verbleibende Gefährdungspotential daher als gering angesehen werden.

Vertraulichkeit: normal

Neben datenschutzrechtlichen Aspekten ginge eine Verletzung der Vertraulichkeit auch immer mit einer möglichen Schädigung der Reputation oder einem Vertrauensverlust von Dritten gegenüber der LUH einher.

⁴ [Schutzstufenkonzept des LfD Niedersachsen](#); PDF vom 25.10.2010

⁵ „IT-Sicherheitskonzept der ZUV für die Gottfried Wilhelm Leibniz Universität Hannover“ (20.12.2017)

Der physikalische Zugriff auf das Veranstaltungsmanagementsystem ANTRAGO ist durch eine protokollierte Zugangskontrolle ausreichend abgesichert.

Die Zugriffe auf die Datenbanken sind technisch nur einem ausgewählten Personenkreis ermöglicht, welcher hinsichtlich des Umgangs mit personenbezogenen Daten sensibilisiert wurde. Die einzelnen Datenbanken sind technisch strikt voneinander getrennt. Die Beschäftigten der Universität sind darüber hinaus generell angehalten, ihre APC durch technische Mittel gegen die Unbefugte Nutzung durch Dritte zu sichern.

Die Administration des Systems und damit der Vollzugriff auf alle Datenbestände sind auf einen bekannten Personenkreis beschränkt. Die Kommunikation zwischen Client und Server erfolgt leider unverschlüsselt, erfolgt aber nur innerhalb des Verwaltungsnetzes. Potentiell könnten hierdurch Informationen auf Protokollebene abgefangen und interpretiert werden, durch den mittleren Schutzbedarf ist der Aufwand hierfür aber hinsichtlich des möglichen Schadens nicht unerheblich und diese Art des Angriffs daher als nicht sehr attraktiv einzuschätzen.

Eine Herausgabe der Daten durch zur Einsicht befugte Personen an unbefugte Dritte oder die Benutzung der Daten zu nicht dafür vorgesehenen Zwecken kann jedoch durch angemessene Maßnahmen nicht gänzlich vermieden werden. Eine besondere Rolle spielt hier auch die Herausgabe an persönlich vertraute, jedoch nicht berechnigte Personen im Rahmen dienstlicher Tätigkeiten.

Integrität: normal

Durch die Verletzung der Integrität der Datenbestände könnten Informationen an dafür nicht vorgesehen Empfänger gelangen (z.B. durch Verfälschung einer Faxnummer). Dies kann auch zu weiterführenden rechtlichen Konsequenzen führen.

Der Übertragungsweg kann als hinreichend gesichert angesehen werden und technische Störungen welche zu einer Verfälschung führen können sind höchst unwahrscheinlich.

Die größte Gefährdung liegt beim Faktor Mensch. Organisatorisch wurde darauf geachtet, dass alle Personen, welche Datensätze manipulieren können, hinreichend auf das System geschult wurden, um Fehlbedienungen auszuschließen.

Für die Mutwillige Änderung von Datensätzen gelten dieselben Aspekte welche schon bei den Schutzzielen Verfügbarkeit und Vertraulichkeit betrachtet wurden.

3. Hosting IuK

3.1 Hardware

Der Server wird virtuell auf einem x64 Bit System unter MS Windows Server betrieben.

3.2 Netzwerk

Das Veranstaltungsmanagementsystem ANTRAGO wird in dem durch das LUIS besonders abgesicherten Verwaltungsnetz betrieben. Ein Zugriff durch Systeme außerhalb der Verwaltung ist nicht möglich. Zugriff zum System haben nur BenutzerInnen innerhalb der Verwaltung mit besonderen Gruppenrechten.

3.3 Software

Das Veranstaltungsmanagementsystem ANTRAGO der Firma RR Software GmbH ist ein ausführbares Programm. Diese Anwendung läuft zentral auf dem Antrago Server (uhv-antrago) Während der Nutzung der Anwendung greifen nur berechtigten BenutzerInnen über eine Verknüpfung auf dieses Programm zu. Es bedarf daher keiner weiteren Software Installation am ClientPCs.

4. Technisch-organisatorische Maßnahmen des Datenschutzes

4.1 Zugangskontrolle

Der Server steht in den Räumen der Telefonzentrale. Zur Einbruchsicherung sind die Fenster der Telefonzentrale mit einbruchshemmendem und kugelsicherem Glas ausgeführt und mit einer Einbruchmeldeanlage versehen.

Die Räume der Telefonzentrale verfügen zusammenfassend in Abwägung von Aufwand und Nutzen über eine angemessene Sicherheit. Problematisch in diesem Zusammenhang kann sein, dass die Administrierenden der ZUV keinen generellen 24x7 Zutritt zu den von Ihnen betreuten Geräten haben. Hinsichtlich der Nachweisbarkeit der Zugänge und der Behandlung verlorener oder gestohlener Schließmedien könnten personalisierte Zutrittsmedien mit zusätzlichem geistigem Identifikationsmerkmal und durchgängige Protokolle über Organisationseinheitsfremde Zutritte die Sicherheit erhöhen.

Durch die geteilte Nutzung der Räume mit anderen Organisationseinheiten besteht eine theoretische Gefahr der Manipulation an den Versorgungen der Racks. Diese kann jedoch nur im Beisein von ausgewählten Bediensteten der Universität mit protokolliertem Zutritt zu den Räumen erfolgen und ist daher als gering anzusehen.

4.2 Datenträgerkontrolle

Im Server kommen nur fest verbaute Festplatten zum Einsatz. Die Entsorgung erfolgt nach Löschung oder (bei Defekt) über zertifizierte Entsorger. Beim BackupSystem (LUIS) kommen auch Bänder als Speichermedien zum Einsatz, die aus dem Bandroboter nur durch BackupSystemadministratoren entfernt werden können. Das BackupSystem ist in einer feuerfesten Zelle mit besonderer Zugangsbeschränkung gesondert verschlossen. Die Speicherung auf den BackupBändern erfolgt nur verschlüsselt, da das Backup mit clientseitiger Verschlüsselung eingerichtet ist.

4.3 Speicherkontrolle

Ein direkter Zugriff auf die Speicher ist nur für SystemadministratorInnen möglich. Die SystemadministratorInnen müssen sich aber zuvor am System authentifizieren und ein Zugang ist nur MitarbeiterInnen des SG12, LuK möglich. Änderungen an der Datenbank werden protokolliert.

4.4 Benutzerkontrolle

Die Benutzung des Veranstaltungsmangementsystems ANTRAGO ist nur nach Authentifizierung durch Benutzername und Kennwort möglich.

4.5 Zugriffskontrolle

Die zugreifbaren Daten sind für jede/n BenutzerIn über die zugehörigen Rollen geregelt. Die Rollenvergabe erfolgt durch AnwendungsadministratorInnen. Die mit den Rollen verbundenen Rechte sind in der Anwendung selbst definiert. Der Zugriff auf das Datenbanksystem ist nur SystemadministratorInnen des SG 12, LuK möglich.

4.6 Übermittlungskontrolle

Es erfolgt keine Datenübermittlung in andere Verfahren oder an andere Stellen.

4.7 Notfallplan

Das System ist virtualisiert. Es wird auf ein Ersatzsystem repliziert und täglich gesichert. Darüber hinaus wird jeweils die Wochenendsicherung zusätzlich aufbewahrt und die Datenbanken zusätzlich auf dem Dateiserver gesichert. Sollten das System und das Ersatzsystem nicht mehr zur Verfügung stehen, könnten das Veranstaltungsmangementsystem ANTRAGO aus den Sicherungen in kurzer Zeit auf einem anderen virtuellen System kurzfristig wiederhergestellt werden. Der Dienst stünde damit bei vorhandenem virtuellem Ersatzsystem auf einem anderen Virtualisierer voraussichtlich eine Stunde nicht zur Verfügung, etwaige Korrespondenz würde um diese Zeit verzögert werden.

5. Datenkategorien

5.1 Personenkreise

Von folgenden Personengruppen werden in Antrago personenbezogene Daten bearbeitet und gespeichert:

Mitarbeiterinnen/Mitarbeiter des Dez. 1, SG 11 - Personalentwicklung und SG 12 – IuK (Benutzerinnen/Benutzer)

interne Teilnehmende (Beschäftigte, ProfessorInnen und Promotionsstudierende der Leibniz Universität Hannover) sowie interne AuftraggeberInnen für bereichsspezifische Maßnahmen

externe Teilnehmende von Kooperationspartnern und anderen niedersächsischen Hochschulen/Universitäten und sonstige externe Personen

DozentInnen und BeraterInnen der Personalentwicklungsangebote (interne und externe Personen)

Ansprechpersonen externer Weiterbildungsträger, KooperationspartnerInnen

Personenbezogene Daten lassen sich in Antrago in systemweite Daten („Personendaten“) und veranstaltungsbezogene Daten („Teilnehmendendaten“) unterteilen.

5.2 Datenkatalog

Übersicht der Datenkategorien/Datenfelder siehe Datenkatalog

5.3 Datenverarbeitung

In Antrago werden Kommunikationsabläufe, die innerhalb des BenutzerInnenteams sowie mit DozentInnen/BeraterInnen/Coaches und Teilnehmenden stattfinden, im Kundeninformationssystem (KIS) getätigt bzw. darin dokumentiert. (Siehe Datenkatalog)

Des Weiteren werden personenbezogene Daten in Wiedervorlagen verarbeitet. (Siehe Datenkatalog)

Weiterhin findet eine Verarbeitung der personenbezogenen Daten in Reports statt (siehe Reportliste).

5.4 Datenarten und Zwecke der Datenverwendung

Kommunikationsdaten:

Die Kommunikationsdaten sind erforderlich für die Organisation und Abwicklung der Qualifizierungsangebote. Bei internen Teilnehmenden werden sie auch für die Einladung von AbsolventInnen zu aufbauenden Qualifizierungen benötigt. Bei DozentInnen bzw. BeraterInnen geht es um die wiederholte Anfrage für ähnliche oder gleiche Themen sowie die Weiterentwicklung der Angebote.

Teilnahmerelevante Personendaten:

Diese Daten sind erforderlich für die Auswahl (Zielgruppenzugehörigkeit). Sie werden zudem für statistische Zwecke sowie für eine zielgruppenspezifische Qualitätsentwicklung der Angebote erhoben.

Veranstaltungsbezogene Teilnehmendendaten:

Diese Daten sind ebenfalls erforderlich für die Auswahl der Teilnehmenden (Registrierung, ob Zielgruppenzugehörigkeit oder Teilnahmevoraussetzungen vorliegen) bzw. die Reihung der InteressentInnen bei Überbelegung.

Eine detaillierte Darstellung der Datenverwendung einzelner Datenfelder ist im Datenkatalog aufgeführt.

5.5 Rechtsgrundlage für Datenspeicherung/-verarbeitung

Datenart	Datenobjekt/Attribute	Rechtsgrundlage
Personendaten – interne Teilnehmende	Antrago-Datensätze/Name, Vorname, dienstliche Kontaktdaten, Tätigkeit, veranstaltungsbezogene Informationen (bspw. Zielgruppenzugehörigkeit, Stellungnahme des Vorgesetzten vorhanden etc), Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	§ 88 NBG i.V.m. §12 NDSG Nach Ausscheiden der MitarbeiterInnen: 9.2 Nds. AktO
Personendaten – interne AuftragnehmerInnen (BeraterInnen/DozentInnen/Coaches)	Name, Vorname, Kontaktdaten, Qualifikation, Tätigkeit, Zielgruppe, Honorar, Handouts, Protokolle, Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	Art. 6 Abs. 1 lit. e) DSGVO iVm. § 3 Abs. 1 Nr. 6, NHG Art. 6 Abs. 1 lit. a) DSGVO
Personendaten – externe AuftragnehmerInnen (BeraterInnen/DozentInnen/Coaches)	Name, Vorname, Kontaktdaten, Qualifikation, Tätigkeit, ggf. Coaching-Profil, Zielgruppe, Honorar, Handouts, Protokolle und Evaluationsergebnisse, Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	Art. 6 Abs. 1 lit. b) DSGVO Art. 6 Abs. 1 lit. a)
Personendaten – externe Teilnehmende	Name, Vorname, dienstliche Kontaktdaten, Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	Art. 6 Abs. 1 lit. e), Abs. 3 DSGVO iVm. § 3 Abs. 1 Nr. 6 NHG.

6. Zugriffsregelungen/Aufgaben/Rollen und Rechte

6.1 Nutzergruppen

Von dem o. g. Personenkreisen hat lediglich der Kreis der BenutzerInnen Zugriff auf das System. Dieser ist in folgende Nutzergruppen unterteilt, die in Antrago in Form von Rollen eingerichtet werden:

SystemadministratorInnen

BenutzerInnen (mehrere Rollen, siehe 5.3)

SystemadministratorInnen sind MitarbeiterInnen des Dez. 1, SG 12.

Benutzer sind ausschließlich Mitarbeiterinnen und Mitarbeiter des Dezernats 1, SG 11, und 13, die in die Veranstaltungsmanagementaufgaben direkt involviert sind.

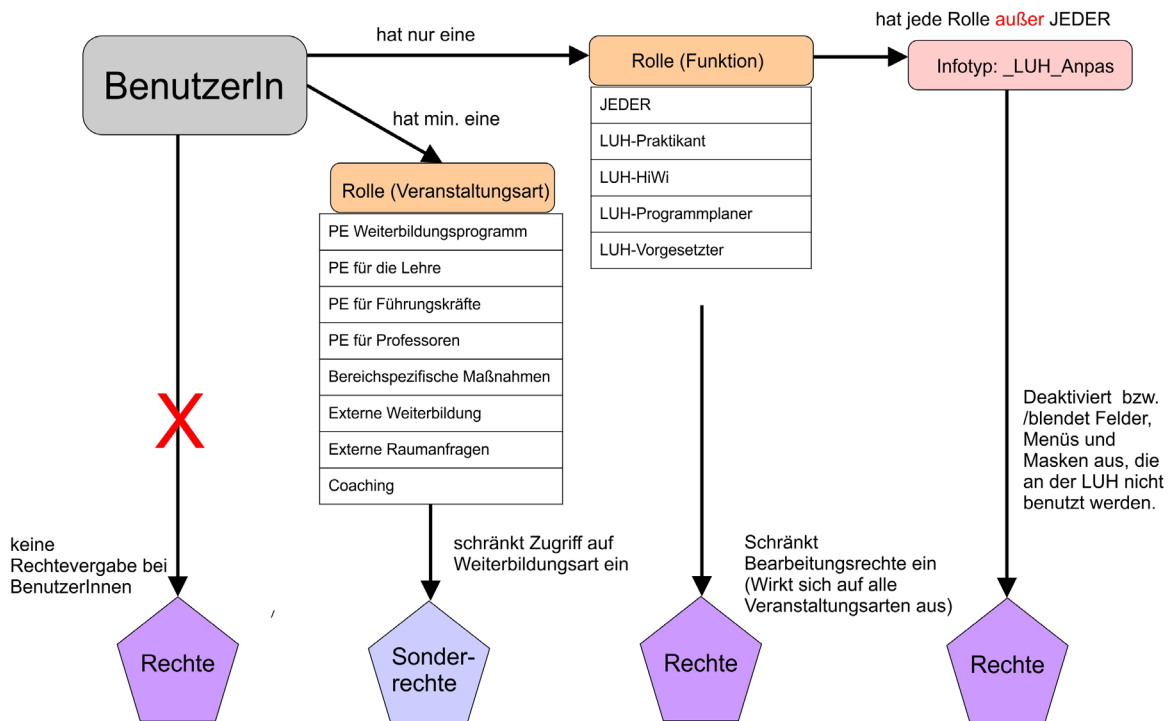
6.2 Rollen und Rechte auf Datenbankebene

Die Rolle SystemadministratorIn hat volle Zugriffsrechte auf Datenbank- und Anwendungsebene. Benutzer-Accounts, die dieser Rolle zugeordnet sind, dürfen stets nur aus entsprechenden Gründen, die den Einsatz eines Systemadministrators zwingend notwendig machen, verwendet werden. BenutzerInnen dieser Rolle unterliegen hohen datenschutzrechtlichen Bestimmungen, die sich aus einem Vertragsverhältnis und einem besonderen Auftrag ergeben müssen.

6.3 Rollen und Rechte auf Anwendungsebene

Alle folgenden Rollen haben ausschließlich Zugriff auf der Anwendungsebene. Der differenzierte Datenzugriff auf Antrago wird über das Rollen- und Rechtekonzept gesteuert. Für die Benutzerinnen und Benutzer sind verschiedene Rollen definiert, deren Zugriffsrechte auf zwei Ebenen gesteuert sind:

1. Bezogen auf Funktionen, die sich aus dem Aufgabenprofil ergeben, z. B. Rollen ProgrammplanerIn,



Studentische Hilfskraft etc.

2. Bezogen auf Veranstaltungsarten, bei denen es sich um in sich abgeschlossene Bereiche des Veranstaltungsmanagements handelt. Diese definieren sich über die Qualifizierungsangebote (bzw. deren Themen bzw. Zielgruppen)

Zu 2. Jede Veranstaltungsart ist in sich abgeschlossen, so dass die darin angebotenen Veranstaltungen von anderen Veranstaltungsarten unabhängig verwaltet werden können:

- Weiterbildungsprogramm
- Personalentwicklung für die Lehre
- Personalentwicklung für Führungskräfte
- Personalentwicklung für Profs
- Bereichsspezifische Maßnahmen
- Coaching
- Externe Weiterbildung
- Externe Raumanfragen (reine Verwaltungsfunktion)

Die BenutzerInnen haben nur für die Veranstaltungsarten Rechte, die für die Aufgabenerfüllung notwendig sind.

Die Veranstaltungsart „Coaching“ unterliegt besonderer Sensibilität. Daher hat nur ein eingeschränkter Benutzerkreis innerhalb der ProgrammplanerInnen darauf Zugriff.

Die Rechte der Rollen sind im Einzelnen in der folgenden Liste einzusehen: Datenkatalog

6.3.1 Rechte für Rolle PraktikantIn

PraktikantInnen nehmen in Antrago lediglich Recherche-Arbeiten vor und haben sehr eingeschränkte, ausschließlich lesende Rechte. Sie können nur veranstaltungsbezogene, nicht jedoch personenbezogene Daten sehen.

Aufgaben in Antrago: Recherchen, Statistiken erstellen und auswerten

6.3.2 Rechte für die Rolle Studentische Hilfskraft:

Studentische Hilfskräfte unterstützen das Sachgebiet Personalentwicklung in vielfältiger Weise und haben daher umfangreiche Berechtigungen im System (in der Regel schreibend). Es handelt sich um eine überschaubare Zahl von drei bis vier Personen, die meist für einen Zeitraum von mehreren Jahren im Sachgebiet Personalentwicklung tätig sind und umfassend in ihre Aufgaben eingearbeitet werden. Mit der Unterzeichnung der „Niederschrift über die förmliche Verpflichtung nicht beamteter Personen“ sind sie zudem hinsichtlich der zu berücksichtigenden Vorschriften unterrichtet.

Aufgaben in Antrago:

Anlegen, Ändern und Löschen von Personen (Teilnehmenden, DozentInnen), Firmen, Veranstaltungsorten und Zuordnung zu Veranstaltungen

Anlegen, Ändern, Löschen von Veranstaltungen/Angeboten/
Veranstaltungsreihen (Themen, Termine, Räume, DozentInnen)

Zu-/Absage von Veranstaltungen/Angeboten/

Veranstaltungsreihen im Namen der ProgrammverwalterInnen (Erstellen von Anschreiben, E-Mails, Listen, Dokumenten) (jedoch ohne Unterschriftsberechtigung)

Erfassen von Anwesenheiten/Evaluationsergebnisse einpflegen

6.3.3 Rechte für ProgrammplanerInnen:

Die ProgrammplanerInnen konzipieren und planen die Qualifizierungsangebote des Sachgebiets Personalentwicklung und werten in diesem Zusammenhang durchgeführte Angebote inhaltlich (Evaluationsergebnisse) sowie statistisch aus. Sie sind in die Verwaltungsprozesse eingebunden. Zudem beraten sie die Beschäftigten bzw. Teams hinsichtlich ihrer Qualifizierungsmöglichkeiten und laden Beschäftigte zielgruppenspezifisch zu den Qualifizierungsangeboten ein. Dazu haben sie umfangreiche schreibende Berechtigungen im System.

Aufgaben in Antrago:

Anlegen, Ändern, Löschen von Personen (Teilnehmenden, DozentInnen), Firmen, Veranstaltungsorten und Zuordnung zu Veranstaltungen

Planen, Anlegen, Ändern, Löschen von Veranstaltungen/Angeboten/
Veranstaltungsreihen (Themen, Termine, Räume, DozentInnen)

Zu-/Absage von Veranstaltungen/Angeboten/

Veranstaltungsreihen (Erstellen von Anschreiben, E-Mails, Listen, Dokumenten)

Erfassen von Anwesenheiten sowie Einpflegen von Evaluationsergebnissen und Auswerten dieser Informationen

Statistische Auswertungen von Anmeldungen/Teilnahme/Zielgruppen/
Bedarfen etc. für Konzeption und Planung von Angeboten

Erstellen von Verteilern für gezielte Einladung einzelner Personen und Personengruppen zu Veranstaltungen (bspw. AbsolventInnen für Folgekurse)

Beratung von Einzelpersonen und Teams unter Einbeziehung absolvierter bzw. durchgeführter Qualifizierungsangebote

6.3.4 Rechte für die Rolle Vorgesetzte

Die Rolle Vorgesetzte erfüllt im Wesentlichen die gleichen Aufgaben wie die ProgrammplanerInnenrolle und hat entsprechende Berechtigungen. Sie hat zusätzlich die Berechtigung, offizielle Dokumente zu unterschreiben

Aufgaben in Antrago:

wie Rolle ProgrammplanerInnen

Unterschrift offizieller Dokumente, z.B. Anschreiben an PR, AuftragnehmerInnenverträge

7. Lösch- und Anonymisierungskonzept

Alle Personen, deren Daten in Antrago verarbeitet werden, werden mittels einer schriftlich verfassten Informationspflicht über folgende Aspekte informiert:

Art der erhobenen Daten

den Zweck der Datenverarbeitung

die Rechtsgrundlage für die Datenverarbeitung

die Verpflichtung für die Bereitstellung

die Widerruflichkeit der Einwilligung

Speicherdauer, Empfänger der personenbezogenen Daten

ihre Betroffenenrechte

Beschwerderecht

DozentInnen, BeraterInnen und Coaches sowie Ansprechpersonen externer Weiterbildungsanbieter haben die Möglichkeit, über eine Einverständniserklärung, ihr Einverständnis in die Speicherung ihrer Daten für einen Zeitraum von 5 Jahren zu geben.

7.1 Fristen für Löschung und Anonymisierung

Datenart	Datenobjekt/Attribute	Löschfrist	Beginn der Löschfrist
Personendaten – interne Teilnehmende	Antrago-Datensätze/Name, Vorname, dienstliche Kontaktdaten, Tätigkeit, veranstaltungsbezogene Informationen (bspw. Zielgruppenzugehörigkeit, Stellungnahme des Vorgesetzten vorhanden etc), Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	6 Jahre	Die Löschfrist der Personendaten beginnt immer zum Zeitpunkt des letzten Veranstaltungstages der zuletzt zugeordneten Veranstaltung.
Personendaten – interne AuftragnehmerInnen (BeraterInnen/DozentInnen/Coaches)	Name, Vorname, Kontaktdaten, Qualifikation, Tätigkeit, Zielgruppe, Honorar, Handouts, Protokolle, Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	1 Jahr bzw. 5 Jahre mit Einverständnis	Die Löschfrist beginnt zum Zeitpunkt des letzten Veranstaltungstages der zuletzt zugeordneten Veranstaltung bzw. bei einer Einwilligung für die 5-jährige Datenspeicherung mit dem Datum der Unterzeichnung.
Personendaten – externe AuftragnehmerInnen (BeraterInnen/DozentInnen/Coaches)	Name, Vorname, Kontaktdaten, Qualifikation, Tätigkeit, ggf. Coaching-Profil, Zielgruppe, Honorar, Handouts, Protokolle und Evaluationsergebnisse, Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	1 Jahr bzw. 5 Jahre mit Einverständnis	Die Löschfrist beginnt zum Zeitpunkt des letzten Veranstaltungstages der zuletzt zugeordneten Veranstaltung bzw. bei einer Einwilligung für die 5-jährige Datenspeicherung mit dem Datum der Unterzeichnung.
Personendaten – externe Teilnehmende	Name, Vorname, dienstliche Kontaktdaten, Kommunikationsabläufe, Reports, Bescheinigungen (siehe Datenkatalog)	1 Jahr	Die Löschfrist der Personendaten beginnt immer zum Zeitpunkt des letzten Veranstaltungstages der zuletzt zugeordneten Veranstaltung.

7.2 Umsetzung der Anonymisierung und Löschung

Die Anonymisierungsfunktionalitäten von Antrago werden nicht genutzt, da Antrago Personendaten bei Personen, die mit mehreren Veranstaltungen verknüpft sind, erst anonymisiert, wenn der Anonymisierungszeitpunkt bei der zuletzt hinzugefügten Veranstaltung eingetreten ist. Wenn die Person fortlaufend für neue Veranstaltungen registriert wird, so erfolgt so lange keine Anonymisierung, bis bei der zuletzt verknüpften Veranstaltung der Anonymisierungszeitpunkt eingetreten ist. Die Historie der Veranstaltungsverknüpfungen der Person bleibt für diesen Zeitraum komplett nachvollziehbar. Dies entspricht nicht den Datenschutzerfordernissen der LUH.

Daher werden abgeschlossene Qualifizierungsangebote vor einer Löschung von Daten statistisch ausgewertet.

Personendaten werden unterschieden nach Teilnehmenden und AuftragnehmerInnen (DozentInnen/BeraterInnen/Coaches) und den entsprechenden Kommunikationsdaten:

Personendaten werden zu Teilnehmerdaten durch eine Verknüpfung der Person mit einer oder mehreren Veranstaltung/en als Teilnehmende. Im Zuge der Registrierung als Teilnehmender werden ergänzende Informationen in Thesauren erfasst.

Personendaten werden zu AuftragnehmerInnendaten durch das Ausfüllen des Antrago-Dozentenformulars. Bei der konkreten Auftragsvergabe entstehen Verknüpfungen der Person mit einer/mehreren

Veranstaltung/en als AuftragnehmerInnen. Es werden ergänzende Informationen in Personen-The-sauren (bspw. Zielgruppe etc.), sowie im Personenfenster auf der Registerkarte „Zusatz“ (Honoraran-gaben) erfasst. Die auftragsbezogenen Honorarinformationen werden bei den Veranstaltungen ge-pflegt.

7.2.1 Vorgehensweise der statistischen Auswertung

Jeweils am 1. Freitag eines jeden Monats um 01:00 Uhr nachts wird über die Windows Aufgabenpla-nung ein definierter SpeedUp Lauf der Antrago- Software (AntragoSpeedup.RRSoftware.exe) gestar-tet, der die abgeschlossenen Veranstaltungen mit dem Status „Abgerechnet“ filtert. Im Verlauf der Auswertung dieser Veranstaltungen werden statistische Daten, die keine Rückschlüsse auf die Perso-nen zulassen, in Form von Listen ausgewertet. Folgende Daten werden pro Veranstaltung statistisch ausgewertet:

Veranstaltungsnummer

Veranstaltungstitel

Kooperationsveranstaltung

Summe: max. zugelassene TN-Zahl

Summe: Veranstaltungstage

Summe: UE

Summe: Anmeldungen

Summe: Zusagen

Summe: Warteliste

Summe: freie Plätze

Summe: Teilnehmende

Summe: Rücktritte

Kursausfall: ja/nein

Summe der Teilnehmenden: pro Einrichtung (bezogen auf die Ebene Fakultät, Dezernat, Zentrale Ein-richtung (nicht Institut/Sachgebiet etc.)

Summe der Teilnehmenden: Geschlecht männlich

Summe der Teilnehmenden: Geschlecht weiblich

Summe der Teilnehmenden: pro Kooperationseinrichtung

Summe der Teilnehmenden: interne Teilnehmende (Beschäftigte)

Summe der internen Teilnehmenden pro Statusgruppe (Wiss. MitarbeiterInnen, MTV, Prof. etc.)

Summe der Teilnehmenden: interne Teilnehmende externem Status pro Statusgruppe (Lehrbeauftragte etc.)

Summe der Teilnehmenden: externe Teilnehmende

Summe der Teilnehmenden: Tätigkeitsfeld Führungskraft

Summe der Teilnehmenden: Tätigkeitsfeld Projektleitung

Summe der Teilnehmenden: Tätigkeitsfeld in der Lehre tätig

Summe der Teilnehmenden: Tätigkeitsfeld Sonstiges

7.2.2 Vorgehensweise der Datenlöschung

Sobald die Löschrfrist der Daten eingetreten ist, werden die entsprechenden Verknüpfungen zwischen den Personen- und Veranstaltungsdaten aufgelöst und erfasste Informationen zur Teilnahme an dem Qualifizierungsangebot bzw. zur Durchführung des Qualifizierungsangebotes gelöscht. Sollte die Per-son keine weiteren Verknüpfungen als TeilnehmerIn oder AuftragnehmerIn haben, so werden die Per-sonendaten komplett gelöscht. Bestehen noch Verknüpfungen mit Veranstaltungen, so werden die er-forderlichen Personendaten bis zur Löschrfrist gespeichert.

Löschung von Personendaten der Teilnehmenden:

Die Löschfristen unterscheiden sich nach internen und externen Teilnehmenden:

Externe Teilnehmende: Datenlöschung nach einem Jahr

Interne Teilnehmende: Datenlöschung nach sechs Jahren (bzw. tw. auch früher)

Jeweils am 1. Freitag eines jeden Monats um 01:00 Uhr nachts wird über die Windows Aufgabenplanung ein definierter SpeedUp Lauf der Antrago- Software (AntragoSpeedup.RRSoftware.exe) unter Berücksichtigung der Löschfristen gestartet. Mittels dieser Abfrage werden die zu löschenden Personendaten der Teilnehmenden ermittelt und automatisch gelöscht.

Löschung von Personendaten der Auftragnehmer:

Die Löschfristen unterscheiden sich nach AuftragnehmerInnen, die das Einverständnis für eine längere Datenspeicherung gegeben haben und denen ohne dieses:

Ohne Einverständnis: Datenlöschung nach einem Jahr

Mit Einverständnis: Datenlöschung nach fünf Jahren

Jeweils am 1. Freitag eines jeden Monats um 01:00 Uhr nachts wird über die Windows Aufgabenplanung ein definierter SpeedUp Lauf der Antrago- Software (AntragoSpeedup.RRSoftware.exe) unter Berücksichtigung der Löschfristen gestartet. Mittels dieser Abfrage werden die zu löschenden Personendaten der AuftragnehmerInnen ermittelt und aufgelistet. Die Löschung von Auftragnehmerdaten erfolgt in Antrago nicht automatisch und muss daher händisch erfolgen.

Löschung von personenbezogenen Daten in Kommunikationsvorgängen mit Teilnehmenden und AuftragnehmerInnen:

Die Löschfristen von personenbezogenen Daten in Kommunikationsvorgängen mit Teilnehmenden und AuftragnehmerInnen sind im Datenkatalog aufgeführt und unterscheiden sich je nach Personengruppe.

Jeweils am 1. Freitag eines jeden Monats um 01:00 Uhr nachts wird über die Windows Aufgabenplanung ein definierter SpeedUp Lauf der Antrago- Software (AntragoSpeedup.RRSoftware.exe) unter Berücksichtigung der Löschfristen gestartet. Mittels dieser Abfrage werden die zu löschenden Kommunikationsdaten ermittelt und automatisch gelöscht.

Die Löschung erfolgt direkt auf der MS-SQL Datenbank. Es werden sämtliche Teilnehmende- bzw. AuftragnehmerInnendaten, sowie die auf diese referenzierenden Datensätze per SQL-Skript gelöscht, sofern hier personenbeziehbare Daten vorgehalten wurden. Kriterium für die Datenlöschung sind das Abreisedatum der letzten verknüpften Veranstaltung. Bei den Teilnehmenden erfolgte eine Datenselektion der betreffenden Datensätze zur Löschung jeweils in Abhängigkeit der extern/intern Kennzeichnung der Teilnehmenden.

8. Risikoanalyse

8.1 Gefahren- und Risikoanalyse

Anhand der im Veranstaltungsmanagementsystem ANTRAGO verarbeiteten Daten und der Umstände und Zwecke der Verarbeitung (s. Fachkonzept und Berichtskonzept) ist nicht erkennbar, dass die Datenverarbeitung eine besondere Gefährdung der Rechte Betroffener hervorrufen könnte. Eine Risikobewertung im Sinne von Art. 35 DSGVO ist daher nicht gesondert vorzunehmen.

Aufgrund der Zuordnung, der in ANTRAGO gespeicherten personenbezogenen Daten zu den Schutzstufen A, B und C (siehe Schutzstufenkonzept der LfD Niedersachsen), wird die Schwere eines möglichen Schadens als geringfügig/überschaubar eingestuft.

Anlage 4 Reportkonzept

Inhaltsverzeichnis

- 1 Einleitung
- 2 Teilnehmende
- 3 AuftragnehmerInnen (DozentInnen, BeraterInnen, Coaches)
- 4 Veranstaltungen

1 Einleitung

Bedingt durch den Anwendungszweck können im Veranstaltungsmangementsystem ANTRAGO unterschiedliche Ausgaben generiert werden. Diese Anschreiben, Listen und Diagramme werden durch Funktionen innerhalb der Applikation entwickelt und genutzt. Ausgabeformate sind dabei bedingt durch technische Notwendigkeiten Word, Excel oder List & Label oder die Ausgabe auf dem Bildschirm.

Die Nutzung der Listen und Reports wird durch das Rollen- und Rechtesystem eingeschränkt. Die Rollen und Berechtigungen werden im Datenschutz-/Löschkonzept und im Datenkatalog beschrieben. Die Praktikantenrolle erhält keine Berechtigung für Listen und Reports, die anderen Rollen erhalten schreibende Rechte.

Statistische Auswertungen der Qualifizierungsangebote enthalten keine personenbezogenen Daten.

2 Teilnehmende

Report/Abfrage	Datenkategorien	Zweck
Verschiedene Anschreiben (Zusage/Absage/Info Warteliste/Info NachrückerInnen Versendung Teilnahmebescheinigung)	Dienstliche Kontaktdaten des/der internen Bearbeiters/Bearbeiterin, dienstliche Kontaktdaten der Teilnehmenden	Veranstaltungsorganisation
Zertifikate, Teilnahmebescheinigungen	Personendaten und Berufsbezeichnung des/der Auftragnehmers/Auftragnehmerin (DozentIn/BeraterIn/Coach), Personendaten des Teilnehmenden	Veranstaltungsorganisation

3 AuftragnehmerInnen (DozentInnen, BeraterInnen, Coaches)

Report /Abfrage	Datenkategorien	Zweck
Anschreiben an AuftragnehmerInnen Veranstaltungszusage/-absage, Anschreiben Vertragsversendung	Dienstliche Kontaktdaten des/der internen Bearbeiters/Bearbeiterin, Kontaktdaten des des/der Auftragnehmers/Auftragnehmerin (DozentIn/BeraterIn/Coach)	Veranstaltungsorganisation
AuftragnehmerInnenvertrag	Auftraggeberin (LUH,vertreten durch),Kontaktdaten des/der Auftragnehmers/Auftragnehmerin (DozentIn/BeraterIn/Coach), Informationen zum Honorar, zur Übernahme von Hotel-/Reisekosten, Veranstaltungstitel	Vertragsabschluss
Honorarabrechnungsfomular	Kontaktdaten des/der Auftragnehmers/Auftragnehmerin (DozentIn/BeraterIn/Coach), Honorarinformationen	Veranstaltungsabrechnung
Liste Einverständniserklärung Datenspeicherung	Kontaktdaten des/der Auftragnehmers/Auftragnehmerin (DozentIn/BeraterIn/Coach)	Verwaltung AuftragnehmerInnenendaten unter Berücksichtigung DSGVO
Liste AuftragnehmerInnen	Personendaten AuftragnehmerInnen, Informationen zu Aufträgen (Thema, Nr, Honorar)	Verwaltung und Planung von Veranstaltungen

4 Veranstaltungen

Report /Abfrage	Datenkategorien	Zweck
Liste mit Anmeldedaten pro Veranstaltung	Personendaten Teilnehmende (Name, Vorname, Titel), Tätigkeit, Dienststelle, Teilnahmethesauren, Anmeldedatum	Zulassungsverfahren bei Überbelegung/Teilnehmendenreihung bzw. Berücksichtigung Teilnahmevoraussetzungen
Anschreiben und Teilnehmerliste für den Personalrat	Dienstliche Kontaktdaten des/der internen Bearbeiters/Bearbeiterin, Personendaten der Teilnehmenden, Dienststelle, Kostenstelle, Tätigkeit, Tel., Prio, Zusage/Ab-sage/Warteliste, Unterschrift der/des Vorgesetzten	Kommunikation mit PR bei Überbelegung von Veranstaltungen
Anwesenheitsliste	Personendaten der Teilnehmenden sowie Dienststelle, Tätigkeit, Tel.	Organisation der Qualifizierungsangebote
Raumvorbereitungszettel	Personendaten des/der Auftragnehmers/Auftragnehmerin (DozentIn/BeraterIn/Coach)	Organisation der Qualifizierungsangebote
Auflistung von Qualifizierungs- und AuftragnehmerInnen-daten	Rahmendaten des Qualifizierungsangebots, Auftragnehmer-Innendaten mit Honorar	Planung, Drucklegung und Organisation der Qualifizierungsangebote
Auflistung aller Veranstaltung inkl. der DozentInnenangabe: - 3 Tage vor Kursbeginn - 1 Woche vor Kursbeginn	Rahmendaten des Qualifizierungsangebots, Auftragnehmer-Innendaten	Organisation der Qualifizierungsangebote
Liste, zur Berechnung der geplanten Kosten (SOLL) und der Ausgaben (IST) pro AuftragnehmerIn und pro Kurs anhand der eingegebenen Kursdaten	Rahmendaten des Qualifizierungsangebots, AuftragnehmerInnen-daten mit Honorar	Planung und Organisation der Qualifizierungsangebote

Anlage 5 Mandanten**Mandantenliste**

Nr.	Mandant
1	Dezernat 1, Organisations- und Personalentwicklung und IuK-Technik

Anlage 6

Darstellung einer Verarbeitungstätigkeit nach Art. 30 DSGVO

Name des Verfahrens:

Veranstaltungsmanagement		
<input checked="" type="checkbox"/> Ersterfassung	<input type="checkbox"/> Änderung	<input type="checkbox"/> Löschung

1. Zwecke der Verarbeitung

Das Veranstaltungsmanagement ANTRAGO schafft die technischen Voraussetzungen für die Planung und Verwaltung von Veranstaltungen, die nicht im Curriculum der Leibniz Universität Hannover verankert sind. Diese Qualifizierungsangebote adressieren im Rahmen der Personalentwicklung allen Beschäftigten der Leibniz Universität Hannover.

Teilnehmende an den Kursen sind daher MitarbeiterInnen, wissenschaftliche und studentische Hilfskräfte, Lehrkräfte für besondere Aufgaben, ProfessorInnen, JuniorprofessorInnen, Promovierende ohne Beschäftigungsverhältnis, Beschäftigte von Kooperationshochschulen und in Ausnahmefällen auch externe Teilnehmende.

2. Kategorien betroffener Personen und Kategorien personenbezogener Daten

Lfd. Nr.	Personenkreis	Datenkategorie
1	MitarbeiterInnen SG 12 – luK (Administration)	NutzerInnenkontodaten
2	MitarbeiterInnen des Dez. 1, SG 11 und SG 13 – Personalentwicklung/Organisationsentwicklung (BenutzerInnen)	s.o.
3	Interne Teilnehmende (Beschäftigte der Leibniz Universität Hannover)	Personenstammdaten, Kontaktdaten, sowie ergänzende Angaben bei Teilnehmendendaten. Mit Teilnehmendendaten verknüpfte Veranstaltungsdaten, Kommunikationsabläufe (s. Datenkatalog)
4	Externe Teilnehmende von Kooperationspartnern und anderen niedersächsischen Hochschulen/Universitäten und sonstige externe Personen	Personenstammdaten, Kontaktdaten, sowie ergänzende Angaben bei Teilnehmendendaten. Mit Teilnehmendendaten verknüpfte Veranstaltungsdaten, Kommunikationsabläufe (s. Datenkatalog)
5	AuftragnehmerInnen (DozentInnen, Coaches und BeraterInnen) der Qualifizierungsangebote (interne und externe Personen)	Personenstammdaten, Kontaktdaten, sowie ergänzende Angaben bei AuftragnehmerInnendaten. Mit AuftragnehmerInnendaten verknüpfte Veranstaltungsdaten, Kommunikationsabläufe (s. Datenkatalog)

6	Ansprechpersonen externer WeiterbildungsträgerInnen, KooperationspartnerInnen	Personenstammdaten, Kontaktdaten, ggfs. Firmendaten, Kommunikationsabläufe
----------	---	--

3. Kategorien von EmpfängerInnen, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich EmpfängerInnen in Drittländern oder internationalen Organisationen

a) Hochschulinterne EmpfängerInnen

Offengelegte Daten (Ifd. Nr. aus 2)	Hochschulinterne EmpfängerInnen
3 - 4	Personalrat der Leibniz Universität Hannover: Informationen zu Teilnehmendendaten zur Ausübung des Mitbestimmungsrechtes.
3 - 4	Interne AuftragnehmerInnen (DozentInnen, Coaches und BeraterInnen): Informationen zu Teilnehmendendaten, die erforderlich sind für die Durchführung des Qualifizierungsangebots
5 - 6	Beschäftigte der LUH (Teilnehmende), externe InteressentInnen: Versendung von Informationsmaterial über Qualifizierungsangebote online oder in Papierform, interne Weitervermittlung von AuftragnehmerInnen (DozentInnen, Coaches und BeraterInnen)
5 - 6	Finanzbuchhaltung: Abrechnung der Qualifizierungsangebote
3	Beschäftigte des SG12 Überprüfung der Teilnahmevoraussetzungen für die Teilnahme an SAP-Schulungen

b) Hochschulexterne EmpfängerInnen innerhalb der EU

Offengelegte Daten (Ifd. Nr. aus 2)	Hochschulexterne EmpfängerInnen innerhalb der EU
3 und 5	Druckereien: Erstellung und Adressierung von Printprodukten zur Bewerbung der Qualifizierungsangebote
3 - 4	Externe AuftragnehmerInnen (DozentInnen, Coaches und BeraterInnen): Informationen zu Teilnehmendendaten, die für die Durchführung des Qualifizierungsangebots erforderlich sind

c) Hochschulexterne EmpfängerInnen außerhalb der EU

Offengelegte Daten (Ifd. Nr. aus 2)	Hochschulexterne EmpfängerInnen außerhalb der EU (Drittländer und internationale Organisationen) in Fällen des Art. 49 Abs. 1 Unterabs. 2 DSGVO einschließlich der Dokumentierung der geeigneten Garantien

4. Fristen für die Löschung von Daten (bei unterschiedlichen Löschfristen laufende Nummer der Datenkategorie angeben oder Verweis auf das Löschkonzept)

s. Datenschutz-/Löschkonzept

5. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO (grob skizzieren oder Anlage II beifügen und auf diese verweisen)

s. Datenschutz-/Löschkonzept

6. Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten

a. Beginn der Verarbeitung

Die Verarbeitung findet bereits statt.

Die Verarbeitung soll ab 31.07.2019 erfolgen.

b. Rechtsgrundlage der Verarbeitung (Art. 5 Abs. 1 a i.V.m. Art. 6 DSGVO)

Die Datenverarbeitung erfolgt aufgrund folgender Rechtsgrundlagen (bei mehreren Rechtsgrundlagen bitte manuell nach Datenkategorie spezifizieren):

andere Rechtsgrundlage (bitte angeben):

s. Datenschutz-/Löschkonzept

c. Rechtsgrundlage für die Übermittlung von Daten an Dritte

<input type="checkbox"/> Datenverarbeitung durch AuftragsverarbeiterInnen nach Art. 28f. DSGVO Name und Anschrift der Auftragsverarbeiterin / des Auftragsverarbeiters: Art der Datenverarbeitung: Bitte geben Sie hier an, welche Datenverarbeitungsprozesse beim Auftragsverarbeiter stattfinden werden (z.B. Speicherung der Daten). <input type="checkbox"/> Die Auftragsverarbeitung ist durch einen schriftlichen Vertrag, der Regelungen zu Aufträgen, Weisungen zu technischen und organisatorischen Maßnahmen und die Zulassung von Unterauftragsverhältnissen enthält, geregelt. Der Vertrag wurde der Datenschutzbeauftragten/dem Datenschutzbeauftragten zur Prüfung vorgelegt.

Datenübermittlung an Dritte innerhalb der EU (Ziffer 3.a des Verzeichnisses):

Zweck der Übermittlung an Auftragnehmende: Organisation und Durchführung der Qualifizierungsangebote
Rechtsgrundlage für die Übermittlung: Art. 6 Abs. 1 lit. e) iVm § 3 Abs. 1 S. 1 Nr. 6 NHG
Schnittstelle für die Übermittlung: per Brief und Download Ticket System
Häufigkeit der Übermittlung: jeweils vor Durchführung des Qualifizierungsangebots
Bei Übermittlung an unterschiedliche Stellen bitte Antwortfelder vor dem Eintrag entsprechend kopieren.

Zweck der Übermittlung an Druckereien: Adressierung von Printprodukten zur Bewerbung der Qualifizierungsangebote
Rechtsgrundlage für die Übermittlung: Art. 6 Abs. 1 lit. e) iVm § 3 Abs. 1 S. 1 Nr. 6 NHG, siehe beigefügter Auftragsverarbeitungsvertrag
Schnittstelle für die Übermittlung: Download Ticket System
Häufigkeit der Übermittlung: jeweils vor dem Druck des Werbemittels des Qualifizierungsangebots
Bei Übermittlung an unterschiedliche Stellen bitte Antwortfelder vor dem Eintrag entsprechend kopieren.

Datenübermittlung an Dritte außerhalb der EU (Ziffer 3.b des Verzeichnisses):

Zweck der Übermittlung:
Rechtsgrundlage für die Übermittlung:
Schnittstelle für die Übermittlung:
Häufigkeit der Übermittlung:
Bei Übermittlung an unterschiedliche Stellen bitte Antwortfelder vor dem Eintrag entsprechend kopieren.

d. Verfahren zur Löschung der Daten (gemäß Ziffer 4 des Verarbeitungsverzeichnisses)

Die Löschung der Daten erfolgt manuell / automatisch wie folgt:
s. Datenschutz-/Löschkonzept

e. Transparenz: Sind Form und Umfang der Verarbeitung für Betroffene erkennbar?

Form der Verarbeitung (mehrere Angaben möglich):

- Die Verarbeitung erfolgt schriftlich.
- Die Verarbeitung erfolgt mit Hilfe automatisierter Verfahren.
- Die Verarbeitung erfolgt formlos (z.B. mündlich oder fernmündlich).

Die Informationspflichten nach Art 12 DSGVO sind bekannt und werden gewährleistet.

7. Für die Verarbeitungstätigkeit innerhalb der Leibniz Universität verantwortliche Stelle (Einrichtung / Fakultät/ Institut)

Einrichtung / Fakultät / Institut:

Dezernat 1 - Organisations- und Personalentwicklung und IuK-Technik , SG 11, Personalentwicklung

Ansprechpartnerin für Rückfragen (Name, Telefonnummer):

Anna Klobuchowski, -19171

8. Regelmäßige Überprüfung

Die Aktualität der Verfahrensbeschreibung wird

jährlich

_____ (anderer Prüfturnus)

überprüft.

Erster Prüftermin (1 Jahr nach Meldung oder bei gravierenden Änderungen):

31.07.2019

Datum und Unterschrift Verantwortlicher (Instituts-/Einrichtungsleitung/Dezernent/Sachgebietsleitung)

Kontrolle durchgeführt, keinen Handlungsbedarf festgestellt

Datum	Name								

Bearbeitungsvermerke (wird durch den Datenschutzbeauftragten ausgefüllt):

1) Weiterer Handlungsbedarf?

2) Wv. gemäß nächstem Prüftermin

Anlage I – Dokumentationshilfe für die Pflichten nach Art. 5 Abs. 2 DSGVO

Name der Verarbeitungstätigkeit:

Veranstaltungsmanagementsystem

A.1. Zusätzliche Angaben bei elektronischer Datenverarbeitung

a. Eingesetzte Hardware

s. Datenschutz-/Löschkonzept

b. Eingesetzte Software

s. Datenschutz-/Löschkonzept

c. Datenminimierung durch datenschutzfreundliche Voreinstellungen:

Die Voreinstellungen sind so konfiguriert, dass möglichst wenige Daten gespeichert werden.

A.2. Risikoanalyse

a. Festlegung des Schutzbedarfes nach Schutzstufenkonzept

Lfd. Nr.	Datenkategorie	Es handelt sich um besonders sensible Daten nach Art. 9 DSGVO	Ungefähre Anzahl der Betroffenen	Festlegung des Schutzbedarfes (normal, hoch, sehr hoch)
1	Personenstammdaten	nein	bis zu 4.500	normal
2	Kontaktdaten	nein	bis zu 4.500	normal
3	ergänzende Daten bei Teilnehmenden und AuftragnehmerInnen	nein	bis zu 4.500	normal
4	verknüpfte Veranstaltungen	nein	bis zu 4.500	normal
5	NutzerInnenkontodaten	nein	10	normal

In der Gesamtschau wird für das Verfahren ein normaler Schutzbedarf festgelegt.

b. Für das Verfahren relevante Risiken:

<u>Risiko</u>	<u>Bedrohung</u>	<u>Potentielle Schwachstellen</u>	<u>Eintrittswahrscheinlichkeit (gering, normal, hoch, sehr hoch)</u>
Hardwareschaden	Vernichtung	Datenträger	Gering (Datensicherungskonzept, Raid-systeme)
Diebstahl	Verlust	Datenträger	Gering (Zutrittskontrolle)
HackerInnen, Viren, Datenmanipulation, menschliches Versagen oder vorsätzliches missbräuchliches Handeln	Veränderung	Datenträger, Netzwerk	Gering (Einsatz von Antivirenschutzsoftware, Zugriffskontrollen, beschränkt auf wenige Personen/AdministratorInnen)
HackerInnen, Datendiebstahl, menschliches Versagen oder vorsätzliches missbräuchliches Handeln, unbeabsichtigte Fehlkonfigurationen	Unbefugte Offenlegung	Datenträger, Netzwerk	Gering (Netzschutz, Verwaltungsnetz, Zugriffskontrolle, wird durch eine geeignete Einarbeitung der administrativ tätigen Verantwortlichen soweit möglich vermieden)
HackerInnen	Unbefugter Zugang	Datenträger, Netzwerk, Zugriff auf Programm	Gering (Zugangskontrolle)
	(bitte ggf. weitere als relevant identifizierte Risiken ergänzen)		

s. Datenschutz-/Löschkonzept

A.3. Erforderlichkeit einer Datenschutz-Folgenabschätzung nach Art 35 DSGVO

Eine Datenschutz-Folgenabschätzung ist nach Art. 35 DSGVO erforderlich.

Die Datenschutz-Folgenabschätzung wurde am _____ unter dem Aktenzeichen _____ durchgeführt.

Eine Risikobewertung im Sinne von Art. 35 DSGVO ist Bestandteil des Datenschutz- und Löschkonzepts.

A.4. Technische und organisatorische Maßnahmen (Datensicherheitsmaßnahmen)

Weitere technische und organisatorische Maßnahmen?

s. Datenschutz-/Löschkonzept

A.5. Bewertung der Maßnahmen im Verhältnis zum Risiko

Ist das durch die technisch organisatorischen Maßnahmen gewährleistete Schutzniveau gegenüber dem Risiko angemessen?

<input checked="" type="checkbox"/> ja	<input type="checkbox"/> nein
--	-------------------------------

Anlage II – Dokumentation der technischen und organisatorischen Maßnahmen i.S.v. Art. 32 DSGVO

s. *Datenschutz-/Löschkonzept*

Name der Verarbeitungstätigkeit:

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- | | |
|---|--|
| <input type="checkbox"/> Alarmanlage

<input type="checkbox"/> Automatisches Zugangskontrollsystem

<input type="checkbox"/> Schließsystem mit Codesperre

<input type="checkbox"/> Biometrische Zugangssperren

<input type="checkbox"/> Lichtschranken / Bewegungsmelder

<input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.)

<input type="checkbox"/> Protokollierung der BesucherInnen

<input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Absicherung von Gebäudeschächten

<input type="checkbox"/> Chipkarten-/Transponder-Schließsystem

<input type="checkbox"/> Manuelles Schließsystem

<input type="checkbox"/> Videoüberwachung der Zugänge

<input type="checkbox"/> Sicherheitsschlösser

<input type="checkbox"/> Personenkontrolle beim PfortnerIn / Empfang

<input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal

<input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |
|---|--|

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | |
|--|---|
| <input type="checkbox"/> Zuordnung von BenutzerInnenrechten

<input type="checkbox"/> Passwortvergabe

<input type="checkbox"/> Authentifikation mit BenutzerInnenname / Passwort

<input type="checkbox"/> Gehäuseverriegelungen

<input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | <input type="checkbox"/> Erstellen von BenutzerInnenprofilen

<input type="checkbox"/> Authentifikation mit biometrischen Verfahren

<input type="checkbox"/> Zuordnung von BenutzerInnenprofilen zu IT-Systemen

<input type="checkbox"/> Einsatz von VPN-Technologie

<input type="checkbox"/> Sicherheitsschlösser |
|--|---|

- | | |
|--|--|
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim PförtnerIn / Empfang |
| <input type="checkbox"/> Protokollierung der BesucherInnen | <input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input type="checkbox"/> Verschlüsselung von mobilen Datenträgern |
| <input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten | <input type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |
| <input type="checkbox"/> Einsatz von Anti-Viren-Software | <input type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input type="checkbox"/> Einsatz einer Hardware-Firewall | <input type="checkbox"/> Einsatz einer Software-Firewall |

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | |
|---|---|
| <input type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input type="checkbox"/> Verwaltung der Rechte durch SystemadministratorInnen |
| <input type="checkbox"/> Anzahl der AdministratorInnen auf das „Notwendigste“ reduziert | <input type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input type="checkbox"/> Einsatz von Aktenvernichtern bzw. DienstleisterInnen (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input type="checkbox"/> Protokollierung der Vernichtung |
| <input type="checkbox"/> Verschlüsselung von Datenträgern | <input type="checkbox"/> Pseudonymisierung personenbezogener Daten, sobald der Zweck dies zulässt |

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- | | |
|--|---|
| <input type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der EmpfängerInnen von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen | |

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- | | |
|--|--|
| <input type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle BenutzerInnenamen (nicht BenutzerInnen-gruppen) | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <input type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | |

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeberin / des Auftraggebers verarbeitet werden können.

- | | |
|--|--|
| <input type="checkbox"/> Auswahl der Auftragnehmerin / des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <input type="checkbox"/> vorherige Prüfung der und Dokumentation der bei der Auftragnehmerin / beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input type="checkbox"/> schriftliche Weisungen an die Auftragnehmerin / den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) | <input type="checkbox"/> Verpflichtung der Mitarbeiter der Auftragnehmerin / des Auftragnehmers auf das Datengeheimnis |
| <input type="checkbox"/> AuftragnehmerIn hat Datenschutzbeauftragte(n) bestellt | <input type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <input type="checkbox"/> Wirksame Kontrollrechte gegenüber der Auftragnehmerin / dem Auftragnehmer vereinbart | <input type="checkbox"/> laufende Überprüfung der Auftragnehmerin / des Auftragnehmers und ihrer / seiner Tätigkeiten |

- Vertragsstrafen bei Verstößen

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- In Hochwassergebieten: Serverräume über der Wassergrenze
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Trennung von Produktiv- und Testsystem

Muster Auftragsverarbeitungsvertrag

Das folgende Muster dient als Hilfestellung für den Entwurf von Auftragsverarbeitungsverträgen gem. Art. 28 DSGVO.

Der Prozess zum Abschluss solcher Verträge ist zwingend einzuhalten: <https://prozesse.zuv.uni-hannover.de/p/portal#model/8850071ff19646d481767d541059ba36;overview>

Bitte beachten Sie, dass Sie die Texte gegebenenfalls anpassen oder um eigene Informationen ergänzen müssen, auch wo dies nicht durch eckige Klammern oder durch gelbe Markierungen angezeigt ist. Das Musterformular ersetzt keine Rechtsberatung im Einzelfall. Wenden Sie sich gegebenenfalls an: datenschutz@uni-hannover.de.

Vertrag zur Datenverarbeitung im Auftrag

Zwischen der Gottfried Wilhelm Leibniz Universität Hannover, vertreten durch das Präsidium, dieses vertreten durch den Präsidenten, dieser vertreten durch den hauptberuflichen Vizepräsidenten, Welfengarten 1, 30167 Hannover - **nachfolgend „Verantwortlicher“ genannt** -

und der

xxx (Firmenname, Vertreter, etc)

xxx (Adresse)

xxx (PLZ und Ort)

- **nachfolgend „Auftragsverarbeiter“ genannt** -

§ 1 Gegenstand und Dauer der Vereinbarung

- (1) Im Rahmen der Leistungserbringung nach der Vereinbarung **... vom ... [Datum]** (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragsverarbeiter mit personenbezogenen Daten umgeht, für die der Verantwortliche als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragsverarbeiters mit den Daten des Verantwortlichen zur Durchführung des Hauptvertrags. Die Rechte und Pflichten des Hauptvertrags bleiben durch diesen Vertrag unberührt.
- (2) Der Auftrag umfasst Folgendes:
xxx

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Verantwortlichen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.
- (3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- (4) Diese Vereinbarung beginnt mit Unterzeichnung dieses Dokuments und endet mit Auftragserledigung oder Kündigung des Hauptvertrags.
- (5) Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein

schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

- (6) Soweit dieser Vertrag von dem der Auftragserteilung zugrundeliegenden Vertrag abweichende Regelungen trifft, gehen die Regelungen des Vertrags zur Datenverarbeitung im Auftrag vor.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

- (1) Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragsverarbeiters:

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):

xxx

Zweck der Datenverarbeitung:

xxx.

(2) Art der personenbezogenen Daten

Gegenstand der Datenverarbeitung sind folgende Datenarten:

Beispiel:

Persönliche Informationen

Titel, Anrede, Vorname, Nachname, E-Mail-Adresse, Telefonnummer

Anschrift

Adresse, PLZ, Stadt, Firma (private Teilnehmer sind auch zugelassen), Branche, Unternehmensgröße, Abteilung

Themenspezifische Informationen

Schulungs-, Dialog-, Projekt oder Veranstaltungsthema sowie besprochene Fragestellungen und Inhalte der Gespräche (Protokolle)

Eine Verarbeitung von besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO oder genetischer, biometrischer Daten oder Gesundheitsdaten gemäß Art. 4 Nr. 13, 14 und 15 DSGVO ist nicht vorgesehen.

(3) Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

xxx

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

- (1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.
- (2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Verantwortlichem und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- (3) Der Verantwortliche hat das Recht, dem Auftragsverarbeiter Weisungen zu erteilen hinsichtlich

der Verarbeitung der personenbezogenen Daten. Der Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

- (4) Der Verantwortliche ist berechtigt, sich wie unter § 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
- (5) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (6) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 4 Weisungsberechtigte des Verantwortlichen, Weisungsempfänger des Auftragsverarbeiters

- (1) Weisungsberechtigte Personen des Verantwortlichen sind:

(Vorname, Name, Organisationseinheit, Telefon)

-
- (2) Weisungsempfänger beim Auftragsverarbeiters sind:

(Vorname, Name, Organisationseinheit, Telefon)

-
- (3) Für Weisung zu nutzende Kommunikationskanäle:

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

-
- (4) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 5 Pflichten des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
- (2) Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt.
- (3) Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Verantwortlichen verarbeiteten Daten von sonstigen Datenbeständen strikt

getrennt werden.

- (4) Die Datenträger, die vom Verantwortlichen stammen bzw. für den Verantwortlichen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
- (5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Er hat die dazu erforderlichen Angaben dem Verantwortlichen unverzüglich an folgende Stelle weiterzuleiten:

(Vorname, Name, Organisationseinheit, Telefon oder E-Mailadresse)

- (6) Der Auftragsverarbeiter führt ab Geltung der DSGVO ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
- (7) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Verantwortlichen nach Überprüfung bestätigt oder geändert wird.
- (8) Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechnete Interessen des Auftragsverarbeiters dem nicht entgegenstehen.
- (9) Unabhängig davon hat der Auftragsverarbeiter personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 und 18 DSGVO zugrunde liegt.
- (10) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder schriftlichen Zustimmung durch den Verantwortlichen erteilen.
- (11) Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Verantwortlichen beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Er verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (12) Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist nur mit Zustimmung des Verantwortlichen gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.
- (13) Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften, insbesondere der DSGVO, des NDSG, BDSG und des Strafgesetzbuchs bekannt sind.

- (14) Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
- (15) Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
- (16) Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz Herr/Frau

...

(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

oder

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

§ 6 Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

- (1) Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.
- (2)

§ 7 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

- (1) Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt.

§ 8 Technische und organisatorische Maßnahmen (insbesondere Art. 28 Abs. 3 Satz 2 lit. c und e DSGVO)

- (1) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen und zu gewährleisten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Der Auftragsverarbeiter garantiert dabei, die in **Anlage xxx** dieses Vertrags spezifizierten und detaillierten technischen und organisatorischen Maßnahmen realisiert zu haben und diese während der Vertragslaufzeit aufrechtzuerhalten. Die in diesem Dokument festgelegten technischen und organisatorischen Maßnahmen sind Bestandteil dieser Vereinbarung.

- (2) Das im Anhang als **Anlage xxx** beschriebene Datenschutz- und Datensicherheitskonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum Datensicherheitsrisiko unter Berücksichtigung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität, Zweckbindung, Transparenz und Intervenierbarkeit detailliert und unter besondere Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar. Der Auftragsverarbeiter passt das Sicherheitskonzept an veränderte Rahmenbedingungen an und stellt eine zeitnahe Realisierung sicher; dem Verantwortlichen ist Gelegenheit zur Überprüfung zu geben. Insbesondere wird der Auftragsverarbeiter seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
- (3) Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (siehe § 8 Abs. 1 und 2) und das Ergebnis samt vollständigem Auditbericht dem Verantwortlichen mitzuteilen.
- (4) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen.
- (5) Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich.
- (6) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über geplante Veränderungen in der Organisation der Datenverarbeitung und den angewandten Verfahren, soweit sie für die Auftragsverarbeitung sicherheitsrelevant sind. Entsprechendes gilt in Fällen von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Der Auftragsverarbeiter stellt sicher, dass die datenschutzrechtlichen Rahmenbedingungen auch bei Einsatz von Telearbeitsplätzen oder mobilem Zugriff seiner Mitarbeitenden auf Datenverarbeitungssysteme oder Daten des Auftragsverarbeiters beachtet werden.
- (7) Die Datensicherheitsmaßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards nicht unterschreiten. Wesentliche Änderungen und Ergänzungen sind vom Auftragsverarbeiter mit dem Verantwortlichen in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.
- (8) Für die Durchführung der Verarbeitung nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Verantwortlichen datenschutzgerecht vernichtet werden. Gleiches gilt für Test- und Ausschussmaterial.
- (9) Sollten Sicherheit oder Verfügbarkeit der Daten bzw. Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse möglicherweise gefährdet sein, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu unterrichten und ihm alle erforderlichen Auskünfte zur Sicherung der Daten selbst sowie ihrer Verfügbarkeit zu erteilen.

(10)

§ 9 Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

- (1) Der Auftragsverarbeiter hat dem Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen sämtliche in ihren Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen datenschutzkonform zu vernichten oder zurückzugeben, sofern nicht nach dem Recht der Europäischen Union oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Datenträger des Auftragsverarbeiters sind danach physisch zu löschen.
- (2) Die Löschung bzw. Vernichtung ist dem Verantwortlichen mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Ein Zurückbehaltungsrecht wird hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen.

§ 10 Haftung

Verantwortlicher und Auftragsverarbeiter haften entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(...ggf. können hier noch abweichende Vereinbarungen getroffen werden)

§ 11 Vertragsstrafe

Bei Verstoß des Auftragsverarbeiters gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird vereinbart, dass der Auftragsverarbeiter an den Verantwortlichen eine Vertragsstrafe von ... Euro zu zahlen hat.

§ 12 Sonstiges

- (1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
- (2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder einem elektronischen Format. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
- (3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Verantwortlichen verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (4) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

Datum:

Unterschriften

Verantwortlicher

Auftragsverarbeiter

Anlagen:

Anlage 1:

Anlage 2: