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 Niedersachen.

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 (IuK). 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	Leibniz Universität Hannover
Prof. Dr. iur. Volker Epping	Elvira Grube
Präsident	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.		
x Ersterfassung	☐Änderung	☐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-MailAnschrift, Tätigkeiten, Gesundheitsdaten
2	Probanden: Studierende	Name, Vorname, Geburtsdatum, Adresse, Telefonnummer, E-MailAnschrift, 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 (lfd. 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 (lfd. 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 (lfd. 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-MailAnschrift, 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:

Risiko	**Bedrohung**	**Potentielle Schwachstellen**	**Eintrittswahrscheinlichkeit (gering, normal, hoch, sehr hoch)**
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.

☐	Alarmanlage	☐	Absicherung von Gebäudeschächten
☐	Automatisches Zugangskontrollsystem	☒	Chipkarten-/Transponder-Schließsystem
☐	Schließsystem mit Codesperre	☐	Manuelles Schließsystem
☐	Biometrische Zugangssperren	☐	Videoüberwachung der Zugänge
☐	Lichtschranken / Bewegungsmelder	☒	Sicherheitsschlösser
☐	Schlüsselregelung (Schlüsselausgabe etc.)	☐	Personenkontrolle beim Pförtner / Empfang
☐	Protokollierung der Besucher	☐	Sorgfältige Auswahl von Reinigungspersonal
☐	Sorgfältige Auswahl von Wachpersonal	☐	Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

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

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

☒ Einsatz von Anti-Viren-Software

☒ Verschlüsselung von Datenträgern in Laptops / Notebooks

☒ Einsatz einer Hardware-Firewall

☒ 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.

☒ Erstellen eines Berechtigungskonzepts

☐ Verwaltung der Rechte durch Systemadministrator

☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☒ Sichere Aufbewahrung von Datenträgern

☒ physische Löschung von Datenträgern vor Wiederverwendung

☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☐ Protokollierung der Vernichtung

☒ Verschlüsselung von Datenträgern

☐ 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.

☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln

☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

☐ E-Mail-Verschlüsselung

☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw.
vereinbarter Löschfristen

☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

☐ 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.

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

6. Auftragskontrolle

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

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

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
- ☐ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Erstellen eines Notfallplans

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☐ In Hochwassergebieten: Serverräume über der Wassergrenze

☐ 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

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, Verlaufsdokumentationen 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 Schweigepflicht[1]. 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 Berufsgeheimnisträger 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 Rechtsmäßigkeit 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 Adminstration 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	Anwendungsadministrator	Anwendender Arzt / Betriebsarzt	Anwender
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			