

MHH Vertraulichkeitserklärung Declaration of Confidentiality

über die Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung und zur Wahrung von Dienst-, Geschäfts- und Privatgeheimnissen

on the obligation to comply with the data protection requirements under the General Data Protection Regulation and to maintain official, business and private secrets.

(nachfolgend Verpflichtete / Verpflichteter) wird in ihrer / seiner Eigenschaft / Funktion als _____ in Kontakt mit sensiblen Daten der Medizinischen Hochschule Hannover (MHH) und deren Beschäftigten kommen. Verpflichtete / Verpflichteter wird hierbei auch Kenntnis von geheimhaltungsbedürftigen Tatsachen erlangen.

(hereinafter referred to as the Obligated Party / Obligated) will come into contact with sensitive data of Hannover Medical School (MHH) and its employees in her / his capacity / function as _____. In doing so, Obligated Party / Obligated will also gain knowledge of facts requiring confidentiality.

Setzt die / der Verpflichtete ihrerseits / seinerseits eigene Mitarbeitende, Dienstleister oder Subunternehmer ein, obliegt ihr / ihm die Pflicht, diesen Personen die Vertraulichkeitserklärung zur Kenntnis zu geben und sie zur Einhaltung der dort aufgestellten Regeln im arbeitsrechtlich zulässigen Rahmen zu verpflichten. Auf Verlangen der MHH hat die / der Verpflichtete den Nachweis in Textform zu erbringen, dass sie / er diese Verpflichtung eingehalten hat.

If the obligated person uses his/her own employees, service providers or subcontractors, he/she is obligated to inform these persons of the confidentiality declaration and to obligate them to comply with the rules set forth therein within the scope permitted by labor law. Upon request of MHH, the obligated party must provide proof in text form that he/she has complied with this obligation.

1. Datenschutz nach DSGVO

Der / Dem Verpflichteten ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen: Personenbezogene Daten müssen

- a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu

1. data protection according to DSGVO (GDPR)

The obligated party is prohibited from processing personal data without authorization. Personal data may only be processed if consent or a legal regulation permits the processing or if processing of such data is mandatory. The principles of the GDPR for the processing of personal data are set out in Article 5 (1) of the GDPR and essentially include the following obligations: Personal data must

- a) be processed in a lawful manner and in a way that is comprehensible to the data subject;
- b) be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- c) adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing ("data minimization");
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal

- treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
- f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Diese Pflichten bestehen auch nach Beendigung der Tätigkeit fort. Sie / Er wird weiter darüber belehrt, dass Verletzungen des Schutzes personenbezogener Daten mit Freiheits- oder Geldstrafe geahndet werden können. Darüber hinaus verpflichtet sich die / der Verpflichtete zur Wahrnehmung des Fernmeldegeheimnisses, sofern § 3 TTDSG sie/ihn hierzu verpflichtet. Geschützt sind ebenfalls Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person sowie Daten in Akten, die offensichtlich aus einer Datei entnommen oder durch automatisierte Verfahren umgeordnet und ausgewertet sind sowie personenbezogene Daten in papiergebundener Form (Aktenführung). Die Wahrung des Schutzes personenbezogener Daten nach den jeweils aktuellen und anwendbaren datenschutzrechtlichen Regelungen der DSGVO, des BDSG und des NDSG ist zu achten.

2. Geheimnisschutz

Die / Der Verpflichtete bestätigt durch ihre / seine Unterschrift die Kenntnisnahme, dass die für die Dauer des auszuführenden Auftrags zugänglichen Daten unter das Datenschutzrecht fallen, wobei insbesondere § 203 Strafgesetzbuch (StGB) und § 59 / § 60 NDSG (Ordnungswidrigkeiten / Straftaten- soweit anwendbar) zu beachten sind und verpflichtet sich,

- Daten und andere Informationen dürfen nicht zu einem anderen als zu dem betrieblichen / vereinbarten Zweck vervielfältigt werden; insbesondere ist es untersagt, das Datenmaterial für private Zwecke und Nebentätigkeiten zu kopieren und / oder an Dritte unbefugt weiterzugeben.
- Es dürfen nur die für die konkrete Aufgabenerfüllung notwendigen Daten abgerufen werden.
- Es ist untersagt, Daten zu verfälschen, unechte Daten herzustellen sowie vorsätzlich unechte oder verfälschte Daten zu gebrauchen.

- data which are inaccurate in relation to the purposes of their processing are erased or rectified without delay; and
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were processed;
- f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage by appropriate technical and organizational measures ("integrity and confidentiality");

These obligations shall continue after the termination of the activity. He/she is further instructed that personal data breach may be punished with imprisonment or a fine. In addition, the obligated party undertakes to observe the secrecy of telecommunications, insofar as Section 3 TTDSG obliges him/her to do so. Also protected are individual data on the personal and factual circumstances of a specific or identifiable natural person, as well as data in files that have obviously been taken from a file or rearranged and evaluated by automated processes, as well as personal data in paper-based form (file management). The protection of personal data in accordance with the current and applicable data protection regulations of the DSGVO, the BDSG and the NDSG must be observed.

2. protection of secrets

The obligor confirms by his/her signature that he/she is aware that the data accessible for the duration of the order to be executed is subject to data protection law, whereby in particular Section 203 of the German Criminal Code (StGB) and Section 59 / Section 60 of the NDSG (administrative offenses / criminal offenses- if applicable) are to be observed and undertakes,

- Data and other information may not be duplicated for any purpose other than the operational / agreed purpose; in particular, it is prohibited to copy the data material for private purposes and secondary activities and / or to pass it on to third parties without authorization.
- Only the data necessary for the specific performance of the task may be retrieved.
- It is prohibited to falsify data, to produce false data and to intentionally use false or falsified data.
- Documents containing personal data must be kept safe from access by unauthorized third parties and the data

- Unterlagen mit personenbezogenen Daten sind sicher vor dem Zugriff unbefugter Dritter aufzubewahren und die Daten immer durch Abschießen der Räumlichkeiten so zu sichern, dass sie keinem Dritten zugänglich sind und kein Unberechtigter Zugang erhalten kann, einschließlich einer Sicherung des PC-Zugangs.

Zum Schutz vertraulicher Informationen ist im Rahmen der zugewiesenen Aufgabe die notwendige Sorgfalt anzuwenden. Festgestellte Mängel sind so schnell wie möglich der MHH zu melden. Auf folgende Bestimmungen wird hingewiesen:

- § 133 Abs. 3 StGB - Verwahrungsbruch
- § 201 Abs. 3 StGB - Verletzung der Vertraulichkeit des Wortes
- § 203 StGB - Verletzung von Privatgeheimnissen
- § 204 StGB - Verwertung fremder Geheimnisse
- § 353b StGB - Verletzung des Dienstgeheimnisses
- § 4 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

3. Umgang mit vertraulichen Informationen

Die / Der Verpflichtete schützt und sichert vertrauliche Informationen mit der erforderlichen Sorgfalt, zumindest aber mit der Sorgfalt, mit welcher sie/er eigene vergleichbare Informationen schützt. Vertrauliche Informationen dürfen nur für Zwecke der Bearbeitung im Rahmen der Geschäftsbeziehung verwendet werden, in deren Zusammenhang sie bekannt geworden sind, nicht jedoch für Zwecke Dritter oder für eigene Zwecke. Unterlagen und Datenträger, die vertrauliche Informationen enthalten, dürfen nur mit ausdrücklicher vorheriger Genehmigung des Berechtigten aus den Geschäftsräumen verbracht oder transportiert werden. Werden solche Unterlagen und Datenträger nicht mehr benötigt, sind sie derart zu vernichten, dass ihre Rekonstruktion nicht möglich ist.

Vertrauliche Informationen sind insbesondere alle Informationen, alle wissenschaftlichen, wirtschaftlichen, technischen und sonstigen Daten, Mitteilungen, Schriftstücke und ähnliches, einschließlich textlicher, tabellarischer, grafischer, fotografischer, technischer, zeichnerischer, elektronischer, mündlicher oder sonstiger Aufzeichnungen und Mitteilungen sowie Computersoft- und -hardware, soweit sie in einem Bezug zur MHH stehen sowie sämtliche die MHH selbst betreffenden, nicht öffentlich bekannten Informationen, wie etwa deren Buchhaltung, Rechtsstreitigkeiten oder ähnliches, insbesondere auch Forschungsdaten (auch von Drittmittelprojekten), Geschäftsgeheimnisse, Produkte, Herstellungsprozesse, Know-how, Erfindungen, geschäftliche Beziehungen, Geschäftsstrategien, Businesspläne, Finanzplanung, Personalangelegenheiten sowie jegliche

must always be secured by locking the premises in such a way that no third party can access them and no unauthorized person can gain access to them, including securing PC access.

Necessary care shall be taken to protect confidential information within the scope of the assigned task. Any deficiencies found are to be reported to MHH as soon as possible. Attention is drawn to the following provisions:

- Section 133 (3) StGB - Breach of custody.
- § 201 para. 3 StGB - breach of confidentiality of the word
- § 203 StGB - Violation of private secrets
- § 204 StGB - exploitation of another's secrets
- § 353 b StGB - violation of official secrets
- § 4 Act on the Protection of Business Secrets (GeschGehG)

3. Handling of confidential information

The obligor shall protect and safeguard confidential information with the necessary care, or at least with the care with which he/she protects his/her own comparable information. Confidential information may only be used for the purposes of processing within the framework of the business relationship in connection with which it became known, but not for the purposes of third parties or for the Obligor's own purposes. Documents and data carriers containing confidential information shall be only be removed from the business premises or transported with the express prior consent of the authorized party. If such documents and data carriers are no longer required, they shall be destroyed in such a way that their reconstruction is not possible.

Confidential information is in particular all information, all scientific, economic, technical, and other data, communications, written documents, and the like, including textual, tabular, graphic, photographic, technical, drawing, electronic, oral, or other records and communications, as well as computer software and hardware, as far as they are related to MHH, as well as all information concerning MHH itself that is not publicly known, such as its accounting, legal disputes or the like, in particular also research data (also of third-party funded projects), business secrets, products, manufacturing processes, know-how, inventions, business relationships, business strategies, business plans, financial planning, personnel matters, as well as any documents and information which are the subject of technical and organizational secrecy measures and are marked as confidential or are to be regarded as confidential according to the nature of the

Unterlagen und Informationen, die Gegenstand technischer und organisatorischer Geheimhaltungsmaßnahmen sind und als vertraulich gekennzeichnet oder nach der Art der Information oder den Umständen der Übermittlung als vertraulich anzusehen sind. Keine vertraulichen Informationen sind solche Informationen, die der Öffentlichkeit vor der Mitteilung oder Übergabe durch den Inhaber bekannt oder allgemein zugänglich waren oder dies zu einem späteren Zeitpunkt ohne Verstoß gegen eine Geheimhaltungspflicht werden; die dem Empfänger bereits vor der Offenlegung durch den Inhaber und ohne Verstoß gegen eine Geheimhaltungspflicht nachweislich bekannt waren; die von dem Empfänger ohne Nutzung oder Bezugnahme auf vertrauliche Informationen von dem Inhaber selber gewonnen wurden; oder die dem Empfänger von einem berechtigten Dritten ohne Verstoß gegen eine Geheimhaltungspflicht übergeben oder zugänglich gemacht werden.

Die / Der Verpflichtete darf vertrauliche Informationen offenlegen, wenn sie / er hierzu aufgrund eines Gesetzes, einer Verordnung oder einer behördlichen Weisung in einem Gerichts- oder Verwaltungsverfahren verpflichtet ist. Dies aber mit der Maßgabe, dass die / der Verpflichtete die MHH über diese Verpflichtung vor der Offenlegung informiert, zumutbare Mittel des Rechtsschutzes und der verfahrensrechtlichen Sicherung der Geheimhaltung ausschöpft und nur insoweit vertrauliche Informationen veröffentlicht, wie die oben genannte hoheitliche Verpflichtung reicht. Die Verpflichtungen zur Vertraulichkeit bestehen noch weitere zehn Jahre nach Beendigung des Informationsaustausches zum oben genannten Zweck fort.

4. Erweiterter Geheimnis- und Sicherheitsschutz

Die Verpflichtung zur Verschwiegenheit hinsichtlich Betriebs- und Geschäftsgeheimnissen besteht über die Beendigung der Tätigkeit hinaus zeitlich unbefristet, soweit gesetzlich zulässig und kein anderer Zeitraum ausdrücklich vereinbart ist. Forschungsdaten und sonstige vertrauliche Informationen sind für die Dauer von 5 Jahren nach Vertragsbeendigung geheim zu halten, sofern sie als vertraulich gekennzeichnet sind oder sich dies aus den Umständen ergibt.

Die / Der Verpflichtete ist darüber hinaus zur Verschwiegenheit über sämtliche Informationen verpflichtet, die im Zusammenhang mit dem Krisenmanagement der Einrichtung bekannt werden. Hierzu zählen insbesondere Notfall-, Alarm-, Einsatz-, Evakuierungs-, Pandemie-, Katastrophenschutz-, Wiederanlauf- und Kontinuitätsplanungen sowie Informationen über Krisenstäbe, Zuständigkeiten, Abläufe und

information or the circumstances of the transmission. Not confidential information is such information which was known or generally accessible to the public prior to its disclosure or transfer by the Owner or which becomes so at a later point in time without breach of a confidentiality obligation; which was demonstrably known to the Recipient prior to its disclosure by the Owner and without breach of a confidentiality obligation; which was obtained by the Recipient without use of or reference to confidential information from the Owner itself; or which is transferred or made accessible to the Recipient by an authorized third party without breach of a confidentiality obligation.

The Obligor(s) may disclose Confidential Information if obligated to do so by law, regulation or official directive in a judicial or administrative proceeding. However, this is subject to the proviso that the obligor informs MHH of this obligation prior to disclosure, exhausts reasonable means of legal protection and procedural safeguarding of confidentiality, and discloses confidential information only to the extent that the aforementioned sovereign obligation extends. The confidentiality obligations shall continue to exist for a further ten years after termination of the information exchange for the above-mentioned purpose.

4. Extended Confidentiality and Security Protection

The obligation of confidentiality regarding trade and business secrets shall continue indefinitely beyond the termination of employment, insofar as permitted by law and unless another period has been expressly agreed. Research data and other confidential information must be kept confidential for a period of 5 years following the termination of the contract, provided that they are marked as confidential or that this is apparent from the circumstances.

The Obligor is also obliged to maintain confidentiality regarding all information that comes to their knowledge in connection with the organisation's crisis management. This includes, in particular, emergency, alarm, operational, evacuation, pandemic, civil protection, recovery and business continuity plans, as well as information regarding crisis management teams, responsibilities, procedures and decision-making processes. Disclosure to third parties is only permitted

Entscheidungsprozesse. Eine Offenlegung an Dritte ist nur zulässig, soweit eine gesetzliche Verpflichtung hierzu besteht oder eine ausdrückliche schriftliche Freigabe durch die MHH vorliegt.

Die / Der Verpflichtete ist ferner zur Verschwiegenheit über technische, organisatorische und personelle Schutzmaßnahmen verpflichtet, die dem Schutz von Personen, Gebäuden, Einrichtungen, Informationen, Forschungsdaten oder sonstigen Vermögenswerten der MHH dienen. Dies umfasst insbesondere Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrollen sowie sonstige Sicherheits- und Schutzkonzepte.

Ebenfalls unterliegen sämtliche Informationen zur IT-Sicherheit der MHH der Vertraulichkeit. Hierzu gehören insbesondere Netzwerk- und Systemarchitekturen, Netzwerkpläne, Sicherheitskonzepte, Standorte kritischer Infrastruktur, Server- und Rechenzentrumsinformationen, Informationen über eingesetzte Hard- und Software, Konfigurationsdaten, Schwachstellen, Sicherheitsvorfälle, Notfallmaßnahmen, Wiederherstellungsverfahren, Authentifizierungs- und Berechtigungskonzepte sowie sonstige Informationen, deren Offenlegung die Informationssicherheit oder den Betrieb der MHH beeinträchtigen könnte.

Die vorstehenden Informationen gelten unabhängig von einer ausdrücklichen Kennzeichnung als vertraulich, sofern nach ihrer Art oder den Umständen ihrer Bekanntgabe erkennbar ist, dass ein berechtigtes Interesse an ihrer Geheimhaltung besteht.

Die / Der Verpflichtete erklärt, nunmehr hinreichend über die auferlegten Pflichten zum Datenschutz und Geheimnisschutz sowie die Folgen bei Nichtbeachtung unterrichtet zu sein. Sie / Er unterzeichnet diese Vertraulichkeitserklärung und bestätigt gleichzeitig den Empfang einer Abschrift.

where there is a legal obligation to do so or where express written authorisation has been granted by the MHH.

The Obligee is furthermore obliged to maintain confidentiality regarding technical, organisational and personnel security measures designed to protect persons, buildings, facilities, information, research data or other assets of the MHH. This includes, in particular, access, entry, disclosure, input, order, availability and segregation controls, as well as other security and protection concepts.

All information relating to MHH's IT security is also subject to confidentiality. This includes, in particular, network and system architectures, network plans, security concepts, locations of critical infrastructure, server and data centre information, information on hardware and software in use, configuration data, vulnerabilities, security incidents, emergency measures, recovery procedures, authentication and authorisation concepts, and any other information the disclosure of which could compromise information security or the operation of the MHH.

The above information shall be deemed confidential regardless of whether it is expressly marked as such, provided that it is apparent from its nature or the circumstances of its disclosure that there is a legitimate interest in keeping it confidential.

The obligor declares that he/she has now been adequately informed about the obligations imposed on him/her with regard to data protection and the protection of secrets as well as the consequences of non-compliance.

Datum / Unterschrift der / des Verpflichteten

Date / signature