Medizinische Hochschule Hannover

Datenschutzregelungen für IT-Zugänge

Mit der beantragten Zugriffsvereinbarung erhalten Sie Zugriff auf Datenbestände des Informationssystems der Medizinischen Hochschule Hannover. Die in diesem System gespeicherten Daten sind personenbezogen und unterliegen den einschlägigen Datenschutzbestimmungen. Hierzu zählen die Europäische Datenschutzgrundverordnung (EU-DSGVO), das Bundesdatenschutzgesetz (BDSG) und das Niedersächsische Datenschutzgesetz (NSDG). Diese Zugriffsvereinbarung erlaubt es Ihnen, die erhaltenen Daten nur zu Zwecken zu nutzen, die zur Erfüllung Ihrer dienstlichen Aufgaben erforderlich sind (Artikel 83 der EU-DSGVO regelt die Bedingungen für die Verhängung der Geldbußen bei Verstößen).
Als Mitarbeiter, der zu Patientendaten Zugang erhält, unterliegen Sie zusätzlich dem §203 StGB. Die ihnen anvertrauten Geheimnisse dürfen Sie nicht ohne Ermächtigung an unbefugte Dritte weitergeben. Eine Verletzung des Datengeheimnisses wird in den meisten Fällen gleichzeitig eine Verletzung der Amtsverschwiegenheit bzw. einen Verstoß gegen die arbeitsvertragliche Schweigepflicht darstellen, auch kann in ihr zugleich eine Verletzung spezieller Geheimhaltungspflichten liegen. Dies kann eine disziplinarische Verfolgung nach sich ziehen. Die o.g. Pflichten bestehen auch nach Beendigung der Tätigkeit fort.

Eine nicht zulässige Offenlegung der Ihnen überlassenen personenbezogenen Daten stellt auch immer die Übermittlung an E-Mail-Empfänger außerhalb der MHH dar (beispielsweise an einen Drittmittelgeber), wenn diese Daten in der E-Mail oder in einem Dateianhang zur E-Mail unverschlüsselt versendet werden. Die MHH bietet Ihnen zur verschlüsselten E-Mail-Übertragung das Outlook-AddOn Cryptshare an. Dieses ist standardmäßig in jedem Outlook-Client installiert. Dies kann auch über Cryptshare.mh-hannover.de direkt genutzt werden.

Bedenken Sie bitte, dass jede Person, die Ihr Kennwort kennt, unbefugt auf personenbezogene Datenbestände zugreifen kann. Ihre Benutzer-ID und Ihr Kennwort werden nur Ihnen persönlich zugeteilt, eine Weitergabe des Kennwortes an andere ist untersagt. Falls Sie vermuten, dass Ihr Kennwort Dritten bekannt geworden ist, ändern Sie es bitte sofort mit Hilfe der Funktion „Neues Kennwort“ (Strg+Alt+Entf oder über das gelbe i-Icon im Infobereich des Taskleiste). Bitte denken Sie ebenfalls daran in allen weiteren Anwendungen, bei denen Sie die gleiche Benutzername-Kennwort-Kombination nutzen, Ihr Kennwort unverzüglich zu ändern“.

Beim Wegfall der Aufgabenübertragung, das dieser Datenzugriffsvereinbarung zugrunde liegt, sind Sie verpflichtet, das Zentrum für Informations-Management rechtzeitig über das Ende Ihrer Aufgabe zur Verarbeitung dieser Daten in Kenntnis zu setzen. Diese Meldepflicht wird nur im Falle Ihres Austritts aus der MHH vom Personalmanagement übernommen.

Zusatz für Drittmittelprojektleiter: Sofern Mitarbeiterdaten aus Berichten in den Informationssystemen heruntergeladen werden, unterliegen diese nach Ablauf der Aufbewahrungspflicht der Daten nach der EU-DSGVO der Zweckbindung (Art. 47 Satz 2d). Der Zweck ist mit dem Ende eines Projektes erloschen. Allerdings können nach § 257 Handelsgesetzbuch (HGB) Aufbewahrungsfristen von 10 Jahren erforderlich sein. Ausnahmen regelt auch das NDSG im § 6, der die Zweckbindung regelt zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung und zur Durchführung von Organisationsuntersuchungen sowie zu Ausbildungs- und Prüfungszwecken, soweit nicht berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten überwiegen. Nach § 35 BDSG Absatz 3 (gemäß Artikel 18 der EU-DSGVO, Einschränkung der Verarbeitung) können Daten nach Wegfall der Zweckbindung auch gesperrt werden, wenn gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen der Löschung entgegenstehen. Eine Sperrung der heruntergeladenen Daten und der daraus resultierenden Weiterverarbeitungsergebnissen können Sie nur durch eine Verschlüsselung von Dateien vornehmen (beispielsweise Kennwortgeschütze Zip-Archive). Nach Ablauf der Aufbewahrungsfrist ist die unwiederbringliche Löschung der Daten zu veranlassen. Hierzu ist ein geeignetes Nachweisinstrument zu führen. Für die dauerhafte Einhaltung der Schutzmaßnahmen sind Sie verantwortlich.

Ersteller:	Prüfer:	Genehmiger:
Neitz-Kluge, Tatjana	23.08.2018, Weber, Synia Dr.	23.08.2018, Weber, Synia Dr.