Dienstvereinbarung Zutritt

Dienstvereinbarung über die Einführung und den Betrieb von Zutrittskontrollsystemen

zwischen

der Georg-August-Universität Göttingen Stiftung öffentlichen Rechts Universitätsmedizin, vertreten durch den Vorstand,

und

dem Personalrat der Universitätsmedizin Göttingen, vertreten durch die Vorsitzende,

wird nachfolgende Dienstvereinbarung gemäß § 78 NPersVG in Verbindung mit § 67 Abs. 1 Nr. 2 NPersVG geschlossen.

§ 1 Geltungsbereich

(1) Diese Vereinbarung gilt

persönlich

für alle Beschäftigten der Universitätsmedizin Göttingen (UMG)

räumlich

für alle Gebäude und Räume, die durch die UMG genutzt werden und gemäß § 2 dieser Vereinbarung entsprechend abgesichert werden müssen

sachlich

für den Einsatz von IT-Systemen und technischen Einrichtungen zum Zwecke der Zutrittskontrolle zu Räumen, räumlich abgegrenzten Bereichen und Gebäuden oder Gebäudeteilen.

(2) Diese Vereinbarung gilt nicht für Daten, die zu einem anderen Zweck als dem der Zutrittskontrolle im Sinne des § 2 erhoben werden, auch wenn dies mit dem gleichen IT-System geschieht, das Daten zum Zweck der Zutrittskontrolle erfasst (z.B. Zeiterfassung, und Systeme für Parkraumbewirtschaftung). Der Umgang mit diesen Daten wird, auch wenn sie im Zusammenhang mit einer Zutrittskontrolle oder durch das gleiche IT-System erfasst werden, in gesonderten Dienstvereinbarungen geregelt.

§ 2 Zweckbestimmung der Zutrittskontrollsysteme

(1) Der Einsatz der Zutrittskontrollsysteme dient dem Schutz der Beschäftigten, dem Schutz personenbezogener Daten, dem Schutz vor unbefugten Eingriffen in Betriebsabläufe und dem Schutz des Eigentums der Stiftung. Eine Auflistung aller in den Betrieb eines Zutrittskontrollsystems einbezogenen Gebäude, Gebäudeteile und Räume und der dort eingesetzten Zutrittskontrollsysteme ist in der Anlage 1 dargestellt.

Der Personalrat erhält zweimal im Jahr eine Liste aller Controller, an denen Zutrittsleser für die verschiedenen Bereiche angeschlossen sind. Zwischenzeitlich eingetretene Veränderungen (z. B neue Zutritts-Leser) sind dabei farblich zu markieren. Der Personalrat wird zudem immer dann informiert, wenn erstmalig bestimmte Gebäude oder Gebäudebereiche mit Zutrittskontrolle ausgestattet werden sollen.

(2) Leistungs- und Verhaltenskontrollen mittels des Zutrittskontrollsystems sind grundsätzlich nicht zulässig. Daten, die im Arbeitsprozess erfasst werden, dürfen nur in begründeten Fällen nach vorheriger Beteiligung und Zustimmung des Personalrats gem. § 67 Abs. 1 Nr. 2 NPersVG zur Leistungs- oder Verhaltenskontrolle genutzt werden. Zuvor sind diese Fälle der Dienststelle zur Prüfung und zur Weitergabe an den Personalrat vorzulegen.

(3) Im Rahmen der notwendigen Kontrollen von Zutritten zu kritischen Infrastrukturen im G3-7 (Rechenzentren, Datenverteiler, Büro der Bereichsleitung) ist die Geschäftsbereichsleitung des G3-7 und in deren Abwesenheit auch die Vertretung berechtigt, Zutritte zu kritischen Infrastrukturen proaktiv zu überprüfen. Es ist dringend notwendig, dies auch für Wochenenden und Feiertage zu ermöglichen, um eventuellen Missbrauch zeitnah zu erkennen und Karten ggf. sperren zu lassen.
Der Personalrat wird über die erfolgten Überprüfungen monatlich unterrichtet und erhält eine schriftliche Auswertung der getroffenen Maßnahmen. Bei jeder Auffälligkeit, wird der Personalrat umgehend und eigenständig informiert.

(4) Die Vergabe der Transponder/Mitarbeiterkarten und die Verwaltung der damit verbundenen Zutrittsrechte erfolgt ausschließlich nach Kriterien, die sich aus den dienstlichen und arbeitsbezogenen Notwendigkeiten ableiten lassen.

(5) Erkenntnisse, die aus dem Zutrittskontrollsystem unter Verletzung dieser Vereinbarung gewonnen wurden, dürfen nicht verwendet werden. Zur Aufklärung eines begründeten Verdachts auf Straftaten oder schwerwiegende Pflichtverletzungen aufgrund gesetzlicher und behördlicher Verpflichtungen, insbesondere durch staatliche Ermittlungsbehörden, dürfen die personenbezogenen Daten auswertet und verwendet werden. Der Personalrat wird unverzüglich von der Maßnahme unterrichtet.

§ 3 Systembeschreibung

(1) Es wird grundsätzlich zwischen 3 Datenarten unterschieden:

Systemdaten:

Zu den Systemdaten gehören Daten wie Betriebssystemdateien, Programmdateien und Protokolldateien gemäß der besonderen Zweckbindung des § 6 Abs. 4 NDSG.

Zutrittsberechtigungsdaten:

Hierzu gehören Daten wie Identifikationsnummer der Mitarbeiterkarte, räumliche und zeitliche Zuordnung der Zutrittsberechtigungen, Zuordnung der Identifikationsnummer des Transponders/der Mitarbeiterkarten zum Benutzer, Angaben zum Inhaber.

Ereignisdaten:

Hierzu gehören Daten wie Identifikationsnummer der Mitarbeiterkarte, Datum und Uhrzeit des Zutritts und des Verlassens, Terminalnummer des Lesers, Anzahl der Zutrittsversuche.

In der Anlage 2 befindet sich die Beschreibung aller zum Zweck der Zutrittskontrolle erfassten Daten, inklusive der eindeutigen Definition der einzelnen Datenfelder der verschiedenen Datensätze.

(2) Ereignisdaten werden maximal für 3 Monate gespeichert. Sie sind danach eigenständig zu löschen.

Unter Verstoß gegen diese Dienstvereinbarung erfasste Daten und deren Auswertung dürfen grundsätzlich nicht zum Anlass von personalrechtlichen Maßnahmen genommen werden.

Begründete Anträge auf Auswertung personenbezogener Daten von Beschäftigten aus dem Zutrittskontrollsystem müssen der Leitung des Geschäftsbereichs Personal (G3-2) vorgelegt werden. Diese entscheidet in Abstimmung mit dem Personalrat, ob – dem Antrag entsprechend – nach dem Sechs-Augen-Prinzip eine Überprüfung unter Beteiligung des Personalrats, der Personalabteilung und des Datenschutzbeauftragten durch den G3-7 durchgeführt wird.

(3) Die verwendeten Transponder/Mitarbeiterkarte sind so fälschungssicher wie möglich gestaltet; die auf dem Transponder/der Mitarbeiterkarte gespeicherten Daten sind vor unbefugtem Zugriff zu schützen.

(4) Die Lesegeräte sind so beschaffen, dass Lesevorgänge ausschließlich durch den Benutzer in Gang gesetzt werden können. Dieser Lesevorgang muss für die Benutzer erkennbar sein. Automatische Lese- oder sonstige Erkennungsvorgänge, die eine nicht bemerkbare Überwachung ermöglichen, sind auszuschließen.

(5) Aus Anlass der Erstinstallation und zum Einpflegen neuer Nutzer, zur Änderung vorhandener Nutzerdaten sowie zur Löschung nicht mehr benötigter Benutzerdaten dürfen Daten zum Zwecke der Benutzereinrichtung aus dem Personalverwaltungssystem übernommen werden. Dabei dürfen nur die Daten aus dem SAP-Ministamm (DWN01, Anlage 3) übernommen werden. Benutzerdaten, die nicht mehr benötigt werden, sind zu löschen.

(6) Die Arbeitsplätze, die für die Systembetreuung, die Benutzeradministration oder andere Aufgaben an dem Zutrittskontrollsystem eingerichtet sind, werden hinsichtlich Datenschutz, Datensicherheit und Berechtigungsvergabe und -verwaltung genauso wie im Personalverwaltungssystem gesichert.

(7) Daten aus dem Zutrittskontrollsystem dürfen in keiner Form an andere Systeme übergeben werden.

§ 4 Autorisierung des Transponders/der Mitarbeiterkarte gegenüber dem Zutrittskontrollsystem

Auf den verwendeten Transpondern/Mitarbeiterkarten werden für Zwecke der Zutrittskontrolle keine personenbezogenen Daten der Benutzer gespeichert oder ausgelesen. Die Autorisierung gegenüber dem Zutrittskontrollsystem erfolgt ausschließlich über die intern im Transponder/der Mitarbeiterkarte gespeicherte eindeutige Identifikationsnummer.

Beim Auslesen oder Auswerten der Historiendaten darf nur die Identifikationsnummer des Transponders bzw. der Mitarbeiterkarte dargestellt werden. Der Name der Besitzerin/des Besitzers darf nicht angezeigt werden.

§ 5 Betrieb des Systems

(1) Alle Systemfunktionen, die Zugriff auf Protokolldateien oder ein Auslesen oder Auswerten von Ereignisdaten ermöglichen, sind mit einem Doppelpasswort zu versehen.

Dies beinhaltet mindestens ein zweigeteiltes Passwort (mind. 16 Zeichen, Sonderzeichen müssen möglich sein). Es ist nur wirksam, wenn beide Teile nacheinander eingegeben werden. Der erste Teil des Passwortes ist nur dem Systemadministrator bekannt, der zweite Teil nur einer Person des Personalrates.

(2) Der Systemadministrator ist zuständig für Funktion und Technik des Systems. Für Wartungszwecke durch den Softwarelieferanten kann eine entsprechend abgesicherte Fernwartungsverbindung eingerichtet werden.

Sämtliche Zugriffe auf das System sind automatisch zu protokollieren. Die Protokolldateien sind auf Verlangen für den Personalrat einsehbar. Die Darstellung erfolgt in lesbarer, verständlicher Form.

Aus den Protokolldateien muss eindeutig hervorgehen, welche Zugriffe auf die Systemdaten, die Zutrittsberechtigungsdaten und die Ereignisdaten von welchen Personen vorgenommen wurden und welche Aktionen während des Zugriffs in Gang gesetzt und durchgeführt wurden. Andere Verwendungen der Protokolldateien sind unzulässig.

(3) Die Person(en), die mit der Administration der Zutrittsberechtigungsdaten betraut sind, d.h. die Benutzeradministrator(en) sind dem Personalrat zu benennen. Ihre Aufgabe ist die Verwaltung der Zutrittsberechtigungsdaten. Sie haben keine Zugriffsrechte auf die Ereignisdaten. Diese Personen können nicht die Aufgaben des Systemadministrators wahrnehmen.

§ 6 Rechte und Pflichten der Beschäftigten, die am Zutrittskontrollsystem teilnehmen

(1) Jede/r Beschäftigte wird rechtzeitig umfassend und in geeigneter Weise über die Wirkungsweise des Systems (z.B. Verwendung ihrer Daten und die Auswertungsmöglichkeiten) informiert.

Weiterhin erhalten die Beschäftigten, die am Zutrittskontrollsystem teilnehmen, eine schriftliche Mitteilung über alle ihre Person betreffenden gespeicherten Daten zu Beginn des Systembetriebes sowie bei jeder Änderung der in der Anlage 3 genannten Zugangsberechtigungsdaten, wenn sie davon betroffen sind.

Jede/r Beschäftigte hat das Recht, sich die auf seinem/ihrem Transponder/ seiner/ihrer Mitarbeiterkarte gespeicherten Daten bei einer Person, die mit der Administration der Zutrittsberechtigungsdaten betraut ist, darstellen zu lassen. Die Darstellung erfolgt in einer für die Beschäftigten nachvollziehbaren und verständlichen Form.

(2) Die Beschäftigten sind für den bestimmungsgemäßen Gebrauch ihres Transponders/ihrer Mitarbeiterkarte verantwortlich. Der Transponder/die Mitarbeiterkarte darf nicht weitergegeben werden und nicht benutzt werden, um Unbefugten den Zutritt zu ermöglichen. Der Verlust des Transponders/der Mitarbeiterkarte ist unverzüglich, nach feststellen des Verlustes, bei der ständig erreichbaren IT Hotline der UMG anzuzeigen. Der zuständige Benutzeradministrator (s. § 5 Abs.3) wird durch die IT-Hotline ebenfalls umgehend unterrichtet.

(3) Die im Zutrittskontrollsystem gewonnenen Daten dürfen nur bestimmungsgemäß verwendet werden (§ 2).

§ 7 Rechte des Personalrates

(1) Über wesentliche Maßnahmen, die das Zutrittskontrollsystem betreffen, ist der Personalrat rechtzeitig und umfassend zu unterrichten. Rechtzeitig ist die Unterrichtung dann, wenn sie erfolgt, solange noch unterschiedliche Lösungsalternativen im Interesse der/des Beschäftigten berücksichtigt werden können und noch keine betrieblichen oder technischen Sachzwänge geschaffen sind.

(2) Wesentliche funktionelle Erweiterungen und der Einsatz neuer Zutrittskontrollsysteme bedürfen der Zustimmung des Personalrates. Sie werden nach Zustimmung in die Anlagen zu dieser Vereinbarung aufgenommen.

(3) Zu seiner Information hat der Personalrat das Recht, an allen Besprechungen teilzunehmen, die aus Anlass von Änderungen oder Erweiterungen des Zutrittskontrollsystems durchgeführt werden.

(4) Der Personalrat hat im Rahmen seiner allgemeinen Aufgaben ein Informations- und Überwachungsrecht bezüglich der Einhaltung dieser Vereinbarung. Der dazu erforderliche Zugang zu den entsprechenden Systemen und die erforderlichen Informationen sind zu gewähren. Der Systemadministrator ist verpflichtet, dem Personalrat alle Informationen und Kenntnisse, die sich aus dem Betreiben des Systems ergeben bzw. die zum Betrieb notwendig sind, zur Verfügung zu stellen.

Protokollerklärung: Wesentliche Maßnahmen und Erweiterungen im Sinne des § 7 Abs. 1 und 2 sind solche, die das Gepräge des eingeführten Zutrittskontrollsystems erheblich verändern, z. B. über die im Rahmen eines Updates/Upgrades hinausgehende Erweiterung oder Veränderung des Funktionsumfanges.

§ 8 Schlussbestimmungen

(1) Diese Dienstvereinbarung tritt nach Veröffentlichung der Amtlichen Mitteilungen in Kraft.

(2) Sie kann von beiden Seiten mit einer Frist von vier Monaten zum Jahresende, frühestens jedoch zum 01.01.2021 gekündigt werden. Beide Parteien werden sich bemühen, in diesem Fall innerhalb eines halben Jahres eine neue Vereinbarung abzuschließen. Eine einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform.

(3) Dienststelle und Personalrat streben an, die vorliegende Dienstvereinbarungen nach Ablauf von 12 Monaten nach Inkrafttreten zu evaluieren.

(4) Sollten einzelne Bestimmungen dieser Dienstvereinbarung unwirksam oder undurchführbar sein, so wird dadurch die Wirksamkeit der Vereinbarung im Übrigen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der Zielsetzung möglichst nahekommen, die die Vertragsparteien mit der unwirksamen beziehungsweise undurchführbaren Bestimmung verfolgt haben.

(5) Die Anlagen dieser Vereinbarung werden fortlaufend aktualisiert und können im Einvernehmen zwischen Personalrat und Dienststelle aktualisiert oder geändert werden, ohne dass es einer Änderung oder Kündigung dieser Dienstvereinbarung bedarf.

Göttingen, den 17.07.2020

Prof. Dr. Wolfgang Brück
Vorstand Forschung und Lehre
Sprecher des Vorstands

Erdmuthe Bach-Reinert
Vorsitzende des Personalrats

Dr. Martin Siess
Vorstand Krankenversorgung

Jens Finke
Vorstand Wirtschaftsführung
und Administration (komm.)