Dienstvereinbarung über die Einführung und den Betrieb eines Zutritts-/Zugangskontrollsystems zwischen

dem Vorstand des Bereichs Humanmedizin der Universität Göttingen, vertreten durch Herrn G. Zwilling

und

dem Personalrat der Medizinischen Einrichtungen der Universität Göttingen, vertreten durch dessen Vorsitzenden Herrn K. Mosbach

wird nachfolgende Dienstvereinbarung gemäß § 67 Nr.2 in Verbindung mit § 78 Nds.PersVG geschlossen.

§ 1 Geltungsbereich

(1) Diese Vereinbarung gilt

persönlich
für alle Mitarbeiterinnen und Mitarbeiter des Bereiches Humanmedizin der Universität Göttingen;

räumlich
für alle Gebäude und Räume, die durch den Bereich Humanmedizin der Universität Göttingen genutzt werden und gemäß § 2 dieser Vereinbarung entsprechend abgesichert werden müssen;

sachlich
für den Einsatz von EDV-Systemen und technischen Einrichtungen zum Zwecke der Zutritts-/Zugangskontrolle zu Räumen, räumlich abgegrenzten Bereichen und Gebäude oder Gebäudeteilen.

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

§ 2 Zweckbestimmung des Zutritts-/Zugangskontrollsystems

(1) Der Einsatz des Zutritts-/Zugangskontrollsystems dient dem Schutz der Mitarbeiterinnen und Mitarbeiter, dem Schutz personenbezogener Daten, dem Schutz vor unbefugten Eingriffen in Betriebsabläufe und dem Schutz des Eigentums des Landes Niedersachsen. Eine Auflistung aller in den Betrieb eines Zutritts-/Zugangskontrollsystems einbezogenen Gebäude, Gebäudeteile und Räume und der dort eingesetzten Zutritts-/Zugangskontrollsysteme ist in der Anlage 1 dargestellt.

(2) Eine Leistungs- oder Verhaltenskontrolle findet nicht statt. Personenbezogene oder personenbeziehbare Daten, die für eine Leistungs- oder Verhaltenskontrolle geeignet sind, dürfen nicht ausgewertet, in andere Systeme übertragen oder dafür verwandt werden, individuelle Eigenschaften mit Anforderungsprofilen zu vergleichen. Ausgenommen bleibt die Regelung in § 3 Abs. 2 dieser Vereinbarung.

(3) Die Vergabe der Transponder/Chipkarten und die Verwaltung der damit verbundenen Zutritts-/Zugangsrechte erfolgt ausschließlich nach Kriterien, die sich aus den dienstlichen und arbeitsbezogenen Notwendigkeiten ableiten lassen.

(4) Erkenntnisse, die aus dem Zutritts-/Zugangskontrollsystem unter Verletzung dieser Vereinbarung gewonnen wurden, dürfen nicht verwendet werden.

§ 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 § 31 BDSG (§ 10(4) NDSG).

Zutritts-/Zugangsberechtigungsdaten:

Hierzu gehören Daten wie Identifikationsnummer des Transponders/der Chipkarte, räumliche und zeitliche Zuordnung der Zutritts-/Zugangsberechtigungen, Zuordnung der Identifikationsnummer des Transponders/der Chipkarten zum Benutzer, Angaben zum Inhaber

Ereignisdaten:

Hierzu gehören Daten wie Identifikationsnummer des Transponders/der Chipkarte, Datum und Uhrzeit des Zutritts/Zugangs und des Verlassens, Terminalnummer des Lesers, Anzahl der Zutritts-/Zugangsversuche.
Weitere Daten, wie z.B. Zeiterfassungsdaten zählen nicht zu den Ereignisdaten im Sinne dieser Vereinbarung, da sie gemäß § 2 Abs.2 gesondert behandelt werden.

In der Anlage 2 befindet sich die Beschreibung aller zum Zweck der Zutritts-/Zugangskontrolle erfassten Daten inklusive der eindeutigen Definition der einzelnen Datenfelder der verschiedenen Datensätze.

(2) Ereignisdaten werden maximal für 3 Monate gespeichert. Sie sind danach zu löschen. Das Auslesen oder Auswerten von Ereignisdaten (Historienspeicher) ist nur bei begründetem Verdacht auf schwerwiegenden Missbrauch der Zugangsberechtigung oder strafbare Handlungen erlaubt.
Der Personalrat ist in jedem Falle vorher zu beteiligen (vergl. § 5 Abs.1).

(3) Die verwendeten Transponder/Chipkarten sind so fälschungssicher wie möglich gestaltet; die auf dem Transponder/der Chipkarte 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) 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 Zutritts-/Zugangskontrollsystem eingerichtet sind, werden hinsichtlich Datenschutz, Datensicherheit und Berechtigungsvergabe und -verwaltung genauso wie im Personalverwaltungssystem gesichert.

(7) Daten aus dem Zutritts-/Zugangskontrollsystem dürfen in keiner Form an andere Systeme übergeben werden. Der Umgang mit Daten, die zu anderen Zwecken erhoben werden als zur Zutritts-/Zugangskontrolle im Sinne dieser Vereinbarung (z.B. durch ein in das Zutritts-/ Zugangskontrollsystem integriertes Zeiterfassungssystem oder im Rahmen von Parkraumbewirtschaftung), wird durch entsprechende Dienstvereinbarungen geregelt.

§ 4 Autorisierung des Transponders/der Chipkarten gegenüber dem Zutritt-/Zugangskontrollsystem

Auf den verwendeten Transpondern/Chipkarten werden für Zwecke der Zutritts-/ Zugangskontrolle keine personenbezogenen Daten der Benutzer gespeichert oder ausgelesen. Die Autorisierung gegenüber dem Zutritts-/Zugangskontrollsystem erfolgt ausschließlich über die intern im Transponder/der Chipkarte gespeicherte eindeutige Identifikationsnummer.

Beim Auslesen oder Auswerten der Historiendaten darf nur die Identifikationsnummer des Transponders bzw. der Chipkarte dargestellt werden. Der Name des Besitzers/der Besitzerin 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 vom Personalrat beauftragten Person.

(2) Von der Dienststelle wird für das Zutritts-/Zugangskontrollsystem ein Systemadministrator und ein Vertreter benannt. 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 Zutritts-/Zugangsberechtigungsdaten 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 Zutritts-/Zugangsberechtigungsdaten betraut sind, d.h. die Benutzeradministrator(en) sind dem Personalrat namentlich zu benennen. Ihre Aufgabe ist die Verwaltung der Zutritts-/Zugangsberechtigungsdaten. Sie haben keine Zugriffsrechte auf die Ereignisdaten. Diese Personen können nicht die Aufgaben des Systemadministrators wahrnehmen.

§ 6 Rechte und Pflichten der Mitarbeiterinnen und Mitarbeiter, die am Zutritt-/Zugangskontrollsystem teilnehmen

(1) Alle Mitarbeiterinnen und Mitarbeiter werden rechtzeitig umfassend und in geeigneter Weise über die Wirkungsweise des Systems (z.B. Verwendung ihrer Daten und die Auswertungsmöglichkeiten) informiert.

Weiterhin erhalten die Mitarbeiterinnen und Mitarbeiter, die am Zutritts-/Zugangskontrollsystem teilnehmen, eine schriftliche Mitteilung über alle ihre Person betreffenden gespeicherten Daten zu Beginn des Systembetriebes sowie bei jeder Änderung der in der Anlage 2 genannten Zugangsberechtigungsdaten, wenn sie davon betroffen sind.

Jede/r Beschäftigte hat das Recht, sich die auf seinem/ihrem Transponder/der Chipkarte gespeicherten Daten bei einer Person, die mit der Administration der Zutritts-/ Zugangsbechtigungsdaten betraut ist, darstellen zu lassen. Die Darstellung erfolgt in einer für die Mitarbeiterinnen und Mitarbeiter nachvollziehbaren und verständlichen Form.

(2) Die Beschäftigten sind für den bestimmungsgemäßen Gebrauch ihres Transponders/ihrer Chipkarte verantwortlich. Der Transponder/die Chipkarte darf nicht weiter gegeben werden und nicht benutzt werden, um Unbefugten den Zutritt/Zugang zu ermöglichen. Der Verlust des Transponders/der Chipkarte ist unverzüglich beim zuständigen Benutzeradministrator (s. § 5 Abs.3) zu melden.

(3) Die im Zutritt-/Zugangskontrollsystem gewonnenen Daten dürfen nur bestimmungsgemäß verwendet werden (§ 2).

§ 7 Rechte des Personalrates

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

(2) Erweiterungen und der Einsatz neuer Zutritts-/Zugangskontrollsysteme 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 Zutritts-/Zugangskontrollsystems 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.

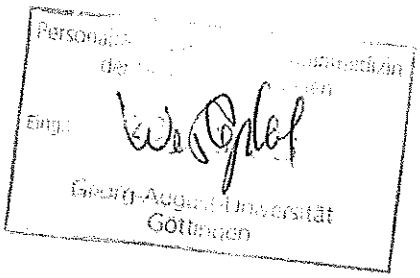
§ 8 Schlussbestimmungen

(1) Diese Vereinbarung tritt am Tage der Unterzeichnung in Kraft.

(2) Sie kann von beiden Seiten mit einer Frist von 6 Monaten zum Jahresende gekündigt werden. In diesem Fall werden sich beide Seite bemühen, innerhalb eines halben Jahres eine neue Vereinbarung abzuschließen.
Eine einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform.
(3) Die Anlagen dieser Vereinbarung werden fortlaufend aktualisiert und können ohne Kündigung dieser Vereinbarung geändert werden. Der Personalrat wird bei jeder Änderung entsprechend § 67 Nds.PersVG beteiligt.

Bereich Humanmedizin
Im Auftrage
i. A.
(Grosse)

Für den Personalrat 14.2.2000
K. Mosbach



Dienstvereinbarung Zutritt

Anlage 3

§ 5, Absatz 3

Systemadministratoren (Windows NT)

Herr Klaus Hauthal	8209
Frau Angelika Scheidel	3458

Systemadministratoren (Datenbank)

Herr Uwe Bischoff	8208
Herr Gerhard Hesse	8202
Herr Günter Neupert	8219

Applikations- / Benutzeradministratoren SIPORT

Herr Frank Körber	3444
Herr Kai Dingenthal	14626

Applikations- / Benutzeradministratoren SAP HR

Herr G. Juretzka	8222
Frau Chr. Schramm-Urbansky	2735

Kartenstellenadministratoren

Frau Claudia Tretzoks	12660
Frau Brigitte Schiele	12661

Georg-August-Universität Göttingen • Stiftung Öffentlichen Rechts
Bereich Humanmedizin • Universitätsklinikum • Medizinische Fakultät

Betriebseinheit Informationstechnologie (BE IT)
Leiter: Bernhard Rassmann

Betriebseinheit Informationstechnologie, Postfach 3742, D-37070 Göttingen

An den

Personalrat
des
Bereichs Humanmedizin
der
Georg-August-Universität Göttingen

im Hause

Applikationsbereich Administration
Leitung: Dr. Günther Juretzka
Adresse: Robert-Koch-Str. 40
D-37075 Göttingen
E-Mail: juretzka
@med.uni-goettingen.de
Telefon: +49-551-39-8222
Fax:: +49-551-39-8234

Bearb.:
E-Mail:
Telefon: +49-551-39-
Ablage:Dokument1
Seiten: 1

Datum: 25. Aug. 2003

Zeiterfassung und Zutrittskontrolle
hier: Änderung der Zuständigkeiten

Sehr geehrte Damen und Herren!

Die Zuständigkeiten für das Zutritts- und Zeiterfassungs-System (SIPORT) haben sich wie folgt geändert:

Frau Haijuan Jin	Tel.: 14626
Herr Frank Körber	Tel.: 3444
Herr Dr. Günther Juretzka	Tel.: 8222

Mit freundlichen Grüßen

Dr. Günther Juretzka