



# Verkündungsblatt

**Herausgeber:** Der Präsident der Tierärztlichen Hochschule Hannover, Bünteweg 2, 30559 Hannover

---

Hannover, 20. Mai 2015      Nr. 212/2015

---

## **Dienstvereinbarung über die Nutzung eines elektronischen Zutrittskontrollsystems an der Stiftung Tierärztliche Hochschule Hannover**

Zwischen der Stiftung Tierärztliche Hochschule (TiHo) und dem Personalrat der Stiftung Tierärztliche Hochschule Hannover (PR) wird auf Grundlage von § 78 des Niedersächsischen Personalvertretungsgesetzes (NPersVG) in Verbindung mit § 67 Abs. 1 Nr. 2 NPersVG folgende Vereinbarung geschlossen:

### **§ 1 Zielsetzung und Allgemeines**

- (1) Die Stiftung Tierärztliche Hochschule Hannover (TiHo) setzt beim Zugang zu den Gebäuden oder Räumen der TiHo ein elektronisches Zutrittskontrollsystem ein, um das Eigentum bzw. die Infrastruktur der TiHo vor Beschädigung, Einbruch und Diebstahl sowie sonstigem schädigendem Verhalten zu schützen und die Sicherheit für die Beschäftigten der Hochschule zu gewährleisten.
- (2) Die Zutrittsberechtigungen zu einzelnen Gebäuden und Räumen werden nach organisatorischen und arbeitstechnischen Notwendigkeiten vergeben. Es soll verhindert werden, dass nicht berechtigte Personen Bereiche der TiHo, die durch derartige Systeme geschützt sind, betreten.
- (3) Es besteht Einigkeit, dass die TiHo nach bestehendem Datenschutzgesetz verpflichtet ist, Datensicherheitsmaßnahmen zu ergreifen, um den Schutz personenbezogener Daten (Anlage 1) vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten.

- (4) Mit dem Zutrittskontrollsystem dürfen keine arbeitsrechtlichen Kontrollen der Beschäftigten durchgeführt werden. Die erzeugten Logfiles dürfen daher ausschließlich für die technische Überprüfung des Systems und im Rahmen von Ermittlungen der Strafverfolgungsbehörden aufgrund begründeter Verdachtsfälle auf strafbare Handlungen verwendet werden. So ist z.B. die Erstellung von Bewegungsprofilen nicht zulässig.

### **§ 2 Geltungsbereich**

- (1) Der räumliche Geltungsbereich dieser Dienstvereinbarung umfasst das elektronische Zutrittskontrollsystem an allen Standorten der TiHo inklusive der Außenstellen.
- (2) In Anlage 2 sind jene Räumlichkeiten angeführt, bei denen zum Zeitpunkt des Abschlusses dieser Dienstvereinbarung bereits ein elektronisches Zutrittskontrollsystem Verwendung findet.
- (3) Sollten nach Abschluss dieser Dienstvereinbarung weitere elektronische Zutrittskontrollsysteme installiert werden bzw. weitere Türen in das vorhandene System einbezogen werden, ist zuvor die Zustimmung des Personalrats einzuholen. Anlage 2 ist entsprechend anzupassen.
- (4) Die Dienstvereinbarung gilt für alle Beschäftigten i.S.d. § 4 NPersVG der TiHo sowie für sonstige in den Betrieb der TiHo eingegliederte Personen, die von der TiHo mit einem elektronischen Schlüssel ausgestattet wurden, um bestimmte Räumlichkeiten der Hochschule über ein elektronisches Schlosssystem betreten zu können.

### **§ 3 Verantwortliche Stelle**

- (1) Verantwortlich für den Betrieb des elektronischen Zutrittskontrollsystems ist die Leitung der Dienststelle. Ihr obliegen die Einrichtung und der ordnungsgemäße Betrieb des elektronischen Zutrittskontrollsystems.
- (2) Die Leitung benennt die mit der Durchführung des Betriebes der elektronischen Zutrittskontrollsysteme betrauten Personen (Anlage 3). Sie stellt durch technische Vorkehrungen sicher, dass nur Berechtigte die Systeme bedienen können.
- (3) Die Leitungen der Hochschuleinrichtungen benennen einen Verantwortlichen und max. 2 Stellvertretungen für ihren Bereich (Anlage 3a). Deren Zugriff dient lediglich der Vergabe der Zugangsberechtigung (Zuordnung von Personen zu bestimmten Türen) für ihre Einrichtung und die evtl. Sperrung bei Kartenverlust.
- (4) Alle verantwortlichen Personen sind in der Anlage 3/3 a namentlich aufzuführen. Änderungen sind der Hochschulleitung und dem Personalrat anzuzeigen.

### **§ 4 Systembeschreibung**

- (1) Beschäftigte erhalten für den Zutritt zu den in Anlage 2 genannten Bereichen eine Zugangsberechtigung, wenn dies zur Erfüllung ihrer Dienstaufgaben notwendig ist. Als Medium für die Authentifizierung für den Zutritt zu den durch elektronische Zutrittskontrollen gesicherten Gebäuden und/oder Räumen wird die TiHo-Karte verwendet. Die Kontrollen werden durch das System Siemens SiPass übernommen. Zu diesem Zwecke werden an den Zugängen zu den unter in Anlage 2 genannten Bereichen Terminals errichtet, die nach Überprüfung der Daten auf der Ausweiskarte den Zutritt frei geben.
- (2) Die Terminals sind so beschaffen, dass sie nur durch den Benutzer „in Gang gesetzt“ werden können. Automatische Aufzeichnungen in Form einer versteckten Überwachung sind dadurch nicht möglich.
- (3) Sowohl die Daten auf der TiHo-Karte als auch die Stamm-Daten des Kontrollsystems beziehen die notwendigen Daten aus dem IDMS der TiHo. Die technischen Details hierzu finden sich in den entsprechenden Dienstvereinbarungen.

- (4) Das an der TiHo verwendete elektronische Zutrittskontrollsystem wird in der Systembeschreibung in Anlage 4 hinsichtlich seiner Funktion beschrieben. Die TiHo hat das Recht, das verwendete System stets auf dem aktuellen Stand der Technik zu halten. Release Wechsel des Zutrittskontrollsystems sind an den Personalrat zu melden. Kommt es dabei zu einer grundlegenden Funktionsänderung des Systems, ist die Zustimmung des Personalrats vor Ein- bzw. Durchführung der Systemänderung einzuholen und Anlage 4 entsprechend anzupassen.

### **§ 5 Transparenz**

- (1) Die Benutzer des Zutrittskontrollsystems der TiHo sind über die Einführung und die wesentlichen Funktionalitäten des elektronischen Zutrittskontrollsystems sowie über den Inhalt dieser Vereinbarung in geeigneter Form zu informieren.
- (2) Den Mitgliedern des Personalrates ist auf Verlangen in die entsprechende Programmdokumentation – soweit diese vom Hersteller der TiHo zur Verfügung gestellt wurde – Einsicht zu gewähren. Zusätzlich haben Vertreter/innen des Personalrats die Möglichkeit, sich das System durch mit dem Betrieb betraute Personen erläutern zu lassen.

### **§ 6 Zugriffsberechtigung und Auswertung**

- (1) Die Daten werden so gespeichert, dass nach Maßgabe von Absatz 2 nur die mit der Wartung und Administration des Zutrittskontrollsystems betrauten Beschäftigten (Anlage 3) darauf Zugriff haben.
- (2) Es besteht Einigkeit, dass das Zutrittskontrollsystem ausschließlich die Zutrittsdaten, nicht aber Austrittsdaten mitprotokolliert.
- (3) Zugriff auf das gesamte Protokoll haben dabei lediglich der von der TiHo beauftragte Hersteller des Zutrittskontrollsystems, sowie die mit der Wartung und Administration des Zutrittskontrollsystems betrauten Beschäftigten (Anlage 3) der TiHo und zwar ausschließlich zum Zweck der technischen Überprüfung sowie für Fehlerbehebungen im System. Diese Daten werden nicht weitergegeben.

- (4) Alle im Zusammenhang mit Zutrittsereignissen ermittelten Daten (Logfiles) werden für einen Zeitraum von höchstens 30 Tagen gespeichert. Spätestens mit Ablauf dieser Frist werden sie gelöscht.
- (5) Falls für sicherheitskritische Bereiche an der TiHo (z. Bsp. für Arbeiten mit Isotopen, zertifizierte Tierversuche, Umgang mit GVOs der Schutzstufen 1 – 3 oder Umgang mit Infektionserregern der Risikogruppen größer gleich 2) abweichende Regelungen getroffen werden sollen, ist der Personalrat an der Definition dieser Regeln für die gesonderten Bereiche zu beteiligen.

## § 7 Personenbezogene Auswertungen

- (1) Personenbezogene Auswertungen der Daten aus dem elektronischen Zutrittskontrollsystem sind ausschließlich für Strafverfolgungsbehörden zulässig. Der Vorgang muss bereits polizeilich zur Anzeige gebracht sein.
- (2) Das Auslesen der Daten erfolgt durch berechtigte Administratoren (Anlage 3) unter Beteiligung des Personalrats und des Datenschutzbeauftragten. Die Weitergabe dieser Daten ist nur an die Strafverfolgungsbehörde zulässig.
- (3) Das Auslesen darf nur dem Zwecke der Klärung der Tatsachen dienen, die als Anlass genannt wurden. Alle gewonnenen Daten, die einer solchen Klärung nicht dienlich sind, werden unverzüglich gelöscht. Die übrigen Daten sind spätestens drei Monate nach Abschluss eines polizeilichen Ermittlungsverfahrens zu löschen.

## § 8 Datenschutz

Die TiHo hat für die Vertraulichkeit der ermittelten personenbezogenen Daten im Sinne des Datenschutzgesetzes zu sorgen. Beschäftigte, die Zugang zu den aufgezeichneten Daten haben, sind hinsichtlich ihrer Geheimhaltungspflichten vom Datenschutzbeauftragten entsprechend zu belehren (Anlage 5).

## § 9 Schlussbestimmungen

- (1) Die Anlagen 1 bis 6 sind Bestandteile dieser Vereinbarung. Aus Gründen der Betriebssicherheit sind die Anlagen vertraulich und werden nicht veröffentlicht.
- (2) Die Dienstvereinbarung tritt am Tage nach ihrer Veröffentlichung im Verkündungsblatt in Kraft.
- (3) Diese Dienstvereinbarung kann beiden Seiten mit einer Frist von vier Monaten - frühestens zwei Jahre nach Inkraftsetzung - schriftlich gekündigt werden. Die Dienstvereinbarung behält im Falle der Kündigung bis zum Abschluss einer neuen Dienstvereinbarung weiter Gültigkeit soweit die Parteien sich nicht auf eine andere vorläufige Regelung einigen.

Hannover, 14.04.2015  
Für die Stiftung Tierärztliche Hochschule  
Hannover  
gez. Dr. Dr. h.c. mult. Gerhard Greif

Hannover, 15.04.2015  
Für den Personalrat  
gez. Birgitt Mendig

Hannover, 20.05.2015

Dr. Dr. h.c. mult. Gerhard Greif  
Präsident

Anlage 1: Personenbezogene Daten

Anlage 2: Standorte mit bestehendem Zutrittskontrollsystem

Anlage 3: Administratoren

Anlage 3a: Dezentrale Personen mit der Berechtigung der Vergabe von Zutrittsberechtigungen in einer Einrichtung

Anlage 4: Systembeschreibungen

Anlage 5: Belehrung durch den Datenschutzbeauftragten

Anlage 6: Verfahrensbeschreibung