

## **Dienstvereinbarung**

### **über die Einrichtung und den Betrieb elektronischer Schließsysteme in den Gebäuden der Universität Regensburg**

Zur Gewährleistung der schutzwürdigen Belange der Beschäftigten, insbesondere vor unzulässigem Gebrauch und unberechtigtem Zugriff auf ihre personenbezogenen Daten, sowie zur Wahrung der berechtigten Interessen der Dienststelle schließen die Universität Regensburg, vertreten durch den Kanzler, und der Personalrat der Universität Regensburg, vertreten durch den Vorsitzenden gemäß Art. 73 i.V.m. Art. 75 a Abs. 1 BayPVG nach Anhörung der Vertrauensperson der schwerbehinderten Menschen und des Gleichstellungsbeauftragten folgende Dienstvereinbarung:

#### **§ 1 Gegenstand und Geltungsbereich**

- (1) Diese Dienstvereinbarung regelt den Einbau und den Betrieb neu zu installierender und bereits vorhandener elektronischer Schließsysteme in den Gebäuden und Räumen der Universität Regensburg. Sie gilt für alle betroffenen Beschäftigten der Universität Regensburg. Personen, die Zugang zu dem jeweiligen System oder dessen Daten haben und nicht Angehörige der UR sind (z.B. Mitarbeiter von Firmen mit Wartungsvertrag), sind durch eine Verpflichtungserklärung zur Einhaltung dieser Dienstvereinbarung zu verpflichten.
- (2) Für jedes elektronische Schließsystem gibt es eine Anlage zu dieser Dienstvereinbarung, in der die jeweiligen Betriebsparameter festgehalten werden. Diese Anlagen sind Bestandteil der Dienstvereinbarung.

#### **§ 2 Zweckbestimmung, Vernetzung**

- (1) Elektronische Schließsysteme werden ausschließlich zur Verbesserung der Sicherheit für Personen, Anlagen und Gegenstände in den Räumlichkeiten der Universität Regensburg sowie zur effizienteren und wirtschaftlicheren Verwaltung von Zutrittsberechtigungen eingesetzt. Es ist untersagt, personenbezogene Daten im Hinblick auf die Erstellung von Anwesenheits- oder Bewegungsprofilen zu sammeln. Eine Leistungs- oder Verhaltenskontrolle der betroffenen Personen findet nicht statt.
- (2) Eine Verknüpfung des Schließsystems einschließlich seiner Daten mit anderen als in der Anlage genannten EDV-Systemen oder Dateien bedarf der erneuten Freigabe und vorherigen Zustimmung des Personalrats.

#### **§ 3 Betrieb der Anlagen**

Verantwortlich für den zentralen Betrieb der elektronischen Schließanlagen ist der Leiter der Technischen Zentrale. Für einzelne Gebäude können in Ausnahmefällen dezentrale Schließanlagen installiert werden.

#### **§ 4 Erfassung, Verwaltung und Auswertung von Daten**

- (1) Alle Beteiligten sind zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet. Vorgesetzte und Organisationsverantwortliche haben auf eine entsprechende Unterrichtung der Mitarbeiter hinzuwirken und die Einhaltung der einschlägigen Vorschriften anzuleiten und laufend zu überwachen.
- (2) Erhebung von Daten  
Es werden ausschließlich die unter Punkt 3 der jeweiligen Anlage zu den einzelnen Schließanlagen genannten Daten erfasst. Die mit einer Zugangskontrolle versehenen Räume sind unter Punkt 2 der jeweiligen Anlage gelistet.

(3) Nutzungsberechtigungen der Daten  
Zugriff auf die personenbezogenen Daten haben lediglich die Personen, die als Administratoren des jeweiligen Schließsystems benannt sind. Sie sind unter Punkt 4 der jeweiligen Anlage gelistet. Die Daten sind vor unbefugtem Zugriff zu schützen.

(4) Auswertungen  
Die Administratoren des Schließsystems sind berechtigt, Zutrittsberechtigungen und Zutrittsprotokolle auszulesen, wenn dies ausschließlich zu technischen Zwecken notwendig ist, wie z. B. bei Wartungsarbeiten, Fehlersuche, Sicherheitstests, Funktionstests. Der Personalrat ist grundsätzlich im Vorfeld über die Erforderlichkeit und die Durchführung von Auslesevorgängen und Auswertungen zu technischen Zwecken zu informieren, in begründeten Ausnahmefällen kann dies auch im Nachgang geschehen. Eine Weitergabe der gewonnenen Daten und darauf basierenden Auswertungen an weitere Personen, die nicht unmittelbar mit der technischen Problemlösung betraut sind, erfolgt nicht. Nach Abschluss der technischen Maßnahmen, spätestens jedoch nach 14 Tagen sind die gewonnenen Daten und darauf basierenden Auswertungen datenschutzrechtlich konform zu löschen bzw. zu vernichten. Eine längere Aufbewahrung zur technischen Problemlösung ist mit der Zustimmung von Datenschutzbeauftragtem und Personalrat in Ausnahmefällen möglich. Auf die Sonderregelungen zu den einzelnen Schließsystemen aufgrund der Anlagen wird hingewiesen.

Eine Datenauswertung zu sonstigen Zwecken ist nur nach Maßgabe von Art. 5 der „Dienstvereinbarung zur Verarbeitung systemimmanenter Daten und der Einsichtnahme in Nutzdaten an der Universität Regensburg“ vom 19./27.03.2018 zulässig.

Sofern bei Wartungs- und Reparaturarbeiten an dem elektronischen Schließsystem den damit beschäftigten Personen Informationen bekannt werden, die gemäß dieser Dienstvereinbarung oder anderen Bestimmungen vertraulich zu behandeln sind, haben sie über den Inhalt Stillschweigen zu bewahren, ebenso über die Erkenntnisse, die Rückschlüsse auf das Verhalten der Systemanwender zulassen könnten.

(5) Schlüsselnutzung  
Die Mitarbeiter/innen sind verpflichtet, mit Schlüsseln oder anderen Zugangsmitteln (z.B. Passwörtern) sorgsam umzugehen und einen etwaigen Schlüsselverlust sofort dem Administrator der Schließanlage (genannt in der jeweiligen Anlage zu dieser Dienstvereinbarung) zu melden.

## **§ 5 Rechte des Personalrats**

- (1) Der Personalrat hat das Recht, die Einhaltung dieser Dienstvereinbarung zu überprüfen. Hierzu erhält er auf Wunsch Einsicht in alle mit dem Betrieb des Systems zusammenhängenden Unterlagen, Protokolle und sonstige Aufzeichnungen.
- (2) Der Personalrat kann nach vorheriger Information der Dienststelle Besichtigungen vor Ort vornehmen.
- (3) Zur Überprüfung der Arbeitsweise des Systems darf der Personalrat mit der Dienststellenleitung Fachleute zu Rate ziehen.
- (4) Bei Einführung, Inbetriebnahme und Änderungen von elektronischen Schließanlagen ist nach Art. 75 a BayPVG der Personalrat mit einzubeziehen.

## **§ 6 Bekanntmachung der Dienstvereinbarung**

- (1) Diese Dienstvereinbarung ist allen betroffenen Personen zugänglich zu machen.
- (2) Die Administratoren des jeweiligen Schließsystems werden zur Einhaltung dieser Dienstvereinbarung schriftlich verpflichtet.

## **§ 7 Inkrafttreten und Geltungsdauer**

- (1) Diese Dienstvereinbarung tritt mit Wirkung vom 01.06.2021 in Kraft. Sie kann mit einer dreimonatigen Frist zum Ende eines Kalendervierteljahres gekündigt werden. Bis zum Abschluss einer neuen Dienstvereinbarung gilt die bisherige Dienstvereinbarung weiter, soweit nicht andere Rechtsvorschriften dem entgegenstehen oder die Parteien sich auf eine vorläufige Regelung einigen.
- (2) Die Anhänge und deren Anlagen können auch ohne Kündigung der Dienstvereinbarung mit Zustimmung des Personalrats geändert werden; die Beteiligungsrechte der Mitarbeitervertretung bleiben hiervon unberührt.
- (3) Mit Inkrafttreten dieser Dienstvereinbarung werden alle bisher abgeschlossenen Dienstvereinbarungen über die Einrichtung und den Betrieb elektronischer Schließsysteme außer Kraft gesetzt.

### Protokollnotiz:

*Eine Auswertung von Daten von Beschäftigten der Universität aus dem vom Studentenwerk Niederbayern/Oberpfalz in den Gebäuden Mensa und Studentenhaus betriebenen elektronischen Schließsystem ist nur nach Maßgabe von Art. 5 der „Dienstvereinbarung zur Verarbeitung systemimmanenter Daten und der Einsichtnahme in Nutzdaten an der Universität Regensburg“ vom 19./27.03.2018 zulässig.*

Regensburg, den 10.05.2021

gez.  
Dr. Christian Blomeyer  
Kanzler der Universität Regensburg

Regensburg, den 12.05.2021

gez.  
Thomas Grimm  
Vorsitzender des Personalrats