

**Dienstvereinbarung
über die Einrichtung und Anwendung eines digitalen Schließsystems
in der Fassung vom 22.11.2017**

zwischen der Universität Passau, vertreten durch den Präsidenten und die Kanzlerin,
und
dem Personalrat der Universität Passau, vertreten durch den Vorsitzenden

§ 1 Gegenstand und Geltungsbereich

- (1) Die Dienstvereinbarung regelt die Einführung und Anwendung eines digitalen Schließsystems (auch Zutrittskontrollsystem genannt).
- (2) Die Dienstvereinbarung gilt für alle Einrichtungen der Universität und alle Beschäftigten im Sinne von Art. 4 BayPVG. Über die Installation von Schließanlagen in weiteren Gebäuden informiert die Universität den Personalrat jeweils schriftlich vor dem Einbau.

§ 2 Zweckbestimmung

- (1) Die Universität setzt das digitale Schließsystem ausschließlich zur Erhöhung der Sicherheit für Personen, Anlagen und Gegenstände in den Gebäuden sowie zur effizienteren und wirtschaftlicheren Verwaltung der Zutrittsberechtigungen ein.
- (2) Das Sammeln von personenbezogenen Daten, z.B. zur Bildung von Bewegungs- oder Anwesenheitsprofilen, mit Hilfe des elektronischen Schließsystems ist unzulässig. Eine Leistungs- und Verhaltenskontrolle der Beschäftigten findet nicht statt.

§ 3 Erhebung, Verarbeitung und Nutzung von Daten

- (1) Das ZIM führt Zutrittsberechtigungen in einer Datenbank der Software des Herstellers auf der Basis von Daten aus dem Identitätsmanagementsystem bzw. durch manuelle Datenpflege. Alle Systemadministratoren erfasst das ZIM in einer Liste. Örtliche Verwalter von Zutrittsberechtigungen haben lediglich Zugriff auf die Zutrittsberechtigungen in ihrem Bereich. Örtliche Verwalter von Zutrittsberechtigungen werden in der jeweiligen Einrichtung in einer Liste erfasst. Die Universität verpflichtet diese Personen durch Unterschrift in den oben genannten Listen, die Dienstvereinbarung einzuhalten.
- (2) Auswertungen nimmt die Universität - außer zu den in Absatz 3 genannten Zwecken - nur bei sicherheitsrelevanten Ereignissen (z. B. Aufenthalt unbekannter Personen in einem Gebäude) und bei Ereignissen von strafrechtlicher Relevanz vor. Nur die Administratoren des Schließsystems dürfen Auswertungen durchführen, informieren davon unverzüglich den Personalrat und die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten und beteiligen sie bzw. ihn an der Auswertung. Über die Auswertung fertigen die Administratoren des Schließsystems ein Protokoll, aus dem sich der Anlass der Auswertung, die auswertenden Personen, der Zeitraum und der Schließbereich ergeben müssen. Das Protokoll ist zusammen mit den anderen Unterlagen zum Schließsystem (Datenschutzrechtliche Freigabe, Liste der Administratoren) am ZIM aufzubewahren. Lediglich das Auswertungsergebnis darf an die Ermittlungsbehörden weitergegeben werden. Alle Daten und Ausdrücke, die einer Klärung nicht dienlich sind, werden unverzüglich gelöscht.
- (3) Die Administratoren des Schließsystems im ZIM bzw. beauftragte Fachfirmen dürfen Zutrittsberechtigungen und Zutrittsprotokolle ohne Beteiligung des Personalrats und der bzw. des Datenschutzbeauftragten lesen, wenn dies ausschließlich zu technischen Zwecken notwendig ist, z. B. bei Wartungsarbeiten, Fehlersuche, Sicherheits- oder Funktionstests.

- (4) Art der gespeicherten Daten und Lösungsfristen sind Teil der Verfahrensbeschreibung (Anlage 1).
- (5) Eine Verknüpfung des Schließsystems ist nur mit dem Identitätsmanagementsystem der Universität (als Quellsystem) zulässig.

§ 4 Rechte des Personalrats

Der Personalrat kann Einsicht in alle mit dem Betrieb des Schließsystems zusammenhängenden Unterlagen, Protokolle und sonstigen Aufzeichnungen verlangen, um die Einhaltung der Dienstvereinbarung zu überprüfen.

§ 5 Inkrafttreten und Geltungsdauer

- (1) Die Dienstvereinbarung tritt mit Unterzeichnung sofort in Kraft.
- (2) Für die Kündigung der Dienstvereinbarung gilt Art. 73 Abs. 4 BayPVG. Die Vertragsparteien müssen unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufnehmen. Bis zum Abschluss einer neuen Dienstvereinbarung gilt die bisherige fort.
- (3) Die Möglichkeit der Vertragsparteien, die Dienstvereinbarung jederzeit in beiderseitigem Einvernehmen zu verändern, bleibt unberührt. Änderungen der Anlagen stimmen die Vertragsparteien außerhalb der förmlichen Änderung der Dienstvereinbarung schriftlich miteinander ab.

Anlage zur Dienstvereinbarung

Art. 27 des Bayerischen Datenschutzgesetzes (BayDSG) bestimmt, dass die behördlichen Datenschutzbeauftragten ein Verzeichnis der bei der öffentlichen Stelle eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, zu führen haben (Verfahrensverzeichnis). Dieses Formular dient sowohl der gemäß Art. 26 Abs. 3 Satz 1 BayDSG erforderlichen Verfahrensbeschreibung als auch der Erstellung des Verzeichnisses. Es fußt auf einem entsprechenden Formular des Bayerischen Staatsministerium des Innern, wurde aber um einige über die gesetzlichen Anforderungen hinausgehenden Punkte erweitert.

Verfahrensbeschreibung

- Erstmalige Beschreibung eines automatisierten Verfahrens**
 Änderung der Verfahrensbeschreibung vom: 08.11.2011

1. Bezeichnung des Verfahrens und allgemeine Angaben

Bezeichnung des Verfahrens (Die Bezeichnung des Verfahrens soll allgemein verständlich sein. Beispiel: „Personaldatei“.)	Stand dieser Verfahrensbeschreibung
Schlüsselfreier Zugang zu verschiedenen Gebäuden und Räumen mittels Zutrittsterminal und der Campuscard an der Universität Passau (Zutrittskontrolle)	17.05.2017
Dienststelle bzw. Dienststellen, in denen das Verfahren eingesetzt wird (Abteilungen / Sachgebiete) (Auch die Dienststelle bzw. die Dienststellen, in denen das Verfahren eingesetzt wird, sind im Klartext zu bezeichnen (z. B. „Einwohnermeldeamt“ oder „Ausländeramt“). Außerdem sollten an dieser Stelle Angaben zur Postanschrift und zur Erreichbarkeit mittels Telefon, Telefax und E-Mail erfolgen.)	
Zutrittsterminals befinden sich an folgenden Standorten der Universität Passau: <ul style="list-style-type: none">- ZIM- IM- ZMK- ITZ- Sportzentrum- NK	
Anlage 1: „Zutrittsterminal Administration“	
Nähere Auskunft erteilt: Gerold Ennser	Nebenstelle: 1816

2. Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung

Aufgaben, zu deren Erfüllung die personenbezogenen Daten erhoben, verarbeitet oder genutzt werden	Rechtsgrundlagen (mit Art.- oder §§-Angabe - Die Rechtsgrundlagen regelmäßiger Datenübermittlungen sind unter Nr. 5 anzugeben.)
<p>Zu den mit Zutrittsterminals gesicherten Türen soll eine im Vorfeld nicht bestimmbare und regelmäßig wechselnde Anzahl von Personen Zutritt erhalten. Durch die Zutrittskontrolle entfällt das Vorhalten von Schlüsseln für diese Türen. So kann bei Verlust oder einer nicht erfolgter Rückgabe eines Schlüssels der Tausch des Türschlosses, der dann aus Sicherheitsgründen erforderlich wäre, vermieden werden, da nur die Berechtigung der Campuscard verändert werden muss, um künftige unberechtigte Zutritte auszuschließen.</p>	<p>Art. 42 Abs. 4 BayHSchG i. V. m. Art. 15 Abs. 1, Art. 16 Abs. 1 und 2, Art. 17 Abs. 1 BayDSG</p>

3. Art der gespeicherten Daten

Lfd. Nr.	Bezeichnung der Daten (es reichen aussagekräftige Oberbegriffe, z.B. Namen, Anschriften; keine Angaben von Feldnummern des Datensatzes)
A a1 a2 a3 a4 a5 a6 a7 a8	<p><u>Auf dem Server für alle Personen gespeicherte allgemeine Daten:</u></p> <p>Systemeigene Nummer, Name, Titel und Namenszusätze</p> <p>CampusCard Nummern</p> <p>Karte Aktiv</p> <p>Berechtigung Zutrittskontrolle</p> <p>Berechtigung Schließfach</p> <p>Bereichsberechtigungen</p> <p>Türberechtigungen</p> <p>Gültigkeitsdauer (Gültig ab: / Gültig bis)</p>
B b1 b2	<p><u>Auf der Campuskarte gespeicherte Daten:</u></p> <p>chipinterne Seriennummer (uid)</p> <p>Benutzernummer</p>
C c1 c2 c3 c4	<p><u>Auf dem Server gespeicherte Buchungsdaten (pro Buchung):</u></p> <p>Datum/Uhrzeit</p> <p>Ereignis (z. B.: „Berechtigter Zutritt“, „Gesperrt keine Zutrittsberechtigung“)</p> <p>Zutrittsterminal</p> <p>Systemeigene Nummer (1)</p>

4. Kreis der Betroffenen

Beschäftigte, Studierende, Gäste und sonstige Personen der Universität Passau, die diesen Dienst nutzen können.

5. Art der regelmäßig zu übermittelnden Daten und deren Empfänger

Lfd. Nr. von Abschnitt 3	Empfänger und Aufgabe, zu deren Erfüllung die Daten übermittelt werden, sowie weitere Angaben zum Empfänger (z. B. öffentliche bzw. nicht-öffentliche Stelle)	Rechtsgrundlage der Übermittlung	automatisiertes Ab-rufverfahren ja/nein	Anlass und Häufigkeit der Übermittlung
a1 – a8	Server für die Zutrittskontrolle an der Universität Passau (verwaltet vom ZIM); Änderung von Datenfeldern durch Übernahme aus dem zentralen Personenverzeichnis (IdM) der Universität Passau Server für die Zutrittskontrolle an der Universität Passau; Manuelle Änderung von Datenfeldern	Behördeninterne Übermittlung, die zum Betrieb des Systems nötig ist	Ja Nein	Änderung von Daten für die beschriebenen Datenfelder. Bei einer Änderung werden die Daten übermittelt.
b1 – b2	Server für die Zutrittskontrolle an der Universität Passau; Buchungsberechtigung ermitteln	Behördeninterne Übermittlung, die zum Betrieb des Systems nötig ist	Ja	Buchung am Zutrittsterminal mit der Campuskarte; die Daten werden pro Buchung an einem Terminal an den Server übermittelt.

6. Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung

Anzugeben ist stets auch der Beginn von Löschungs- bzw. Prüfungsfristen. Beispiel: „Die gespeicherten Daten werden spätestens 3 Jahre nach der vollständigen Rückzahlung des Darlehens gelöscht“.

Jeweils zum 15.6. und 15.12. eines Jahres wird überprüft, welche Personen keine Benutzerkonten mehr im Identity Management System besitzen. Deren personenbezogene Daten a1-a8, b1, b2 werden zur Löschung beim nächsten Regelprüfungstermin vorgemerkt und gelöscht, falls bis dahin keine Reaktivierung der Benutzerkonten erfolgt ist. Die Buchungsdaten (c1-c4) werden nach 7 Tagen gelöscht.

7. Verarbeitungs- und nutzungsberechtigte Personengruppen

(z.B. Verarbeitungs- und nutzungsberechtigt: Sachbearbeiter für im Sachgebiet....., teilnutzungsberechtigt: Sachbearbeiter für im Sachgebiet)

(Beispiel für das Meldewesen einer kreisfreien Stadt: Verarbeitungs- und nutzungsberechtigt: Meldesachbearbeiter, teilnutzungsberechtigt: Sozialhilfesachbearbeiter, Wohngeldsachbearbeiter, Sachbearbeiter der KfZ-Zulassungsstelle, Sachbearbeiter des Ausländeramtes)

Die Zutrittskontrolle an der Universität Passau wird als dezentrales System betrieben. Dadurch können die Daten sowohl global von den Systemadministratoren als auch von der jeweiligen, dem Zutrittsterminal zugeordnete Personen verändert werden.

1. Verarbeitungs- und nutzungsberechtigt:

Systemadministratoren des ZIMs

2. Teilverarbeitung- und nutzungsberechtigt (a1-a8, b2 und c1-c4, aber nur bereichsbezogen): s. Anlage 1 „Zutrittsterminal-Administration“; Teiladministration ist nötig, da das ZIM als zentrale Administration keinen Zugriff auf benötigte Informationen hat, wie z.B. den Personenkreis, der eine Zugangsberechtigung erhalten soll. Es existiert ein Rollensystem, so dass jede/r Verarbeiter/in nur Zugriff auf den in seiner/ihrer Zuständigkeit liegenden Bereich hat.

8. Bei Auftragsdatenverarbeitung: Auftragnehmer

(z.B. AKDB; bei Verfahrensänderung: Unterschied zum bisherigen Verfahren)

Findet eine Auftragsdatenverarbeitung statt: ja

nein

Angaben zum Auftragnehmer:

9. Empfänger vorgesehener Datenübermittlungen in Drittländer

(Staaten außerhalb der EU - Soweit es sich um regelmäßige Datenübermittlungen handelt, sind diese auch in Nr. 5 anzugeben.)

Empfängerstaat:

Empfänger oder Kategorien von Empfängern:

Art der Daten oder Datenkategorien:

Art der vertraglichen Regelungen:

Passau
~~Deggendorf~~

Ort,

17.05.17

Datum,



Unterschrift
Leiter des ZIMs (Thomas Simon)