Staatliche Hochschule
für Gestaltung Karlsruhe

Karlsruhe, 29.09.2021

Vereinbarung zwischen der Staatlichen Hochschule für Gestaltung Karlsruhe und dem Personalrat der Staatlichen Hochschule für Gestaltung Karlsruhe über den Einsatz von elektronischen Schließsystemen

Präambel

Nach Artikel 3 Abs. 2 des Grundgesetzes sind Frauen und Männer gleichberechtigt; alle maskulinen Personen- und Funktionsbezeichnungen in dieser Dienstvereinbarung gelten für Frauen und Männer in gleicher Weise. Die geforderte schriftliche Form für Anträge usw. beinhaltet auch die elektronische Form.

1. Gegenstand und Zweck

Gegenstand dieser Dienstvereinbarung sind die Einführung und der Betrieb einer elektromechanischen Schließanlage auf Basis von „ENIQ Dom Zutrittskontrolle" in den Gebäuden der Staatlichen Hochschule für Gestaltung Karlsruhe sowie die Beteiligung der Beschäftigten und der örtlichen Personalvertretung an diesen Maßnahmen.
Die elektromechanische Schließung soll dazu dienen, dass in Zukunft eine einheitliche Funktionsfähigkeit im Schließsystem geschaffen wird. Wesentliches Merkmal einer solchen Schließung ist die universelle Nutzbarkeit des (einzuführenden) Hochschulausweises durch einfache Programmierung für die Zutrittsberechtigung.
Dieses Schließanlagen-Konzept beinhaltet bei Erweiterungen und Veränderungen sowie bei häufigem Wechsel von Benutzern und Benutzerinnen ein gleichbleibend hohes Sicherheitsniveau.

2. Geltungsbereich

Diese Dienstvereinbarung gilt:

- unmittelbar für alle Bediensteten (Beschäftigte und Beamte) der Staatlichen Hochschule für Gestaltung Karlsruhe im Sinne des § 4 LPVG Baden-Württemberg und darüber hinaus für deren Vorgesetzte;
- für alle Schließsysteme (mechanische und elektronische) in allen von der Hochschule genutzten Gebäuden und Räumen.

3. Systembeschreibung

(1) Das Zutrittssystem besteht aus elektronischen Online- und Offline-Komponente.
- Die Online-Komponenten sind direkt mit dem Zutrittssystem ENIQ/Dom verbunden und werden in erster Linie an Außentüren und Haupteingang Lorenzstr. 15 eingesetzt.
- Die Offline-Komponenten sind nicht mit der Datenbank verbunden und werden in erster Linie an Innentüren eingesetzt.
- Die mechanische Schließanlage wird in erster Linie als Schließung der Haustechnik, Technischen Infrastruktur und Feuerwehr verwendet.

(2) Die Berechtigungen werden in einer Datenbank verwaltet, in der auch die erforderlichen Daten der Hochschulangehörigen gespeichert sind. Die Daten werden von der Personalabteilung und Studierendensekretariat geliefert - definierte Felder siehe Anlage 4.
Die Datenbanksoftware ENIQ/ ELS Pro sowie die vernetzten Komponenten des Schließsystems befinden sich in einem auf einen eigenen Server des Netzwerkes der Hochschule. Notwendige administrative Zugriffe von außen werden durch die IT-Abteilung kontrolliert.

(3) Als Medium zur Identifikation dient ein Mifare-RFID-Chip, der in den (einzuführenden) Hochschulausweis integriert ist. Auf diesem Identmedium sind die Zutrittsberechtigungen gespeichert, Personaldaten sind nicht gespeichert. Das Programm benutzt zur Identifikation die eindeutige Mifare-Nummer und hat eine programmierbare Ablauffrist nach einer definierten Zeit. Danach muss der Nutzer die Zutrittsfreigabe erneut freischalten. Dies geschieht an den Online-Komponenten am Updateterminal. Diese Vorgehensweise ist erforderlich, um einen Schlüsselverlust kurzfristig abzudecken. Veränderungen bei der Zutrittsberechtigung werden an einer speziellen Online-Komponente, einem Updateterminal, erneuert.

(4) Das Programm, das auf die o.g. Datenbanksystem der Schließanlage zugreift, ist mit einem Passwortschutz ausgestattet. Der Programmbereich, der Zutrittsdaten und die entsprechenden Personendaten zeigt (Zutrittslogbuch) ist nur der Rolle „Logbuch" erlaubt. Das Passwort für den Zugriff ist zweigeteilt (Personalrat Rolle „Logbuch"). Alle anderen Rollen können auf diese Daten nicht zugreifen. Das Passwort besteht aus acht Ziffern, wobei der Dienststellenleitung die ersten vier Ziffer bekannt sind und den Personalrat die letzten vier Ziffern.

4. Protokollierung

Im Allgemeinen erfolgt keine Protokollierung in den Offline-Komponenten. Nur für sicherheitsrelevante Räume erfolgt die Protokollierung vor Ort, direkt in der Komponente. Diese Protokolle enthalten keine personenbezogenen Daten. Es wird lediglich die einmalige My-Faire-Kennung des Chips, der sich im Identmedium befindet, gespeichert. Die Verbindung My-Faire-Kennung und Personaldaten kann nicht erfolgen.

5. Verwaltung

Die Datenverarbeitung und die Zuweisung von Zutrittsberechtigungen erfolgt zentral durch einen Mitarbeiter der Zutrittsverwaltung. Die Informationen über die ausgegebenen Identmedien, Personaldaten und Zutrittsberechtigungen sind in einer Datenbank hinterlegt. Zugriff zu dieser Datenbank haben nur die zuständigen Sachbearbeiter.

6. Datensicherung und -löschung

Die gespeicherten Daten der Zutrittskontrolle werden für einen Zeitraum von 90 Tagen gespeichert und danach automatisch gelöscht.

7. Auswertungen

1. Es erfolgt eine anonyme, statistische Auswertung der Schließungen der Offline-Komponenten, die originär von der Firma DOM für Zwecke der Garantiefälle, Reklamationen, Statistiken, Batteriemanagement usw. ohne Transponder-Nummer/MyFAir-Key erhoben/auswertet werden und der Hochschule zum Zwecke des Flächenmanagements dienen.
2. Für eine Genehmigung zum Auswerten personenbezogener Zutrittsdaten sind folgende Voraussetzungen nötig:
   a) Die Antragstellenden müssen darlegen, dass im betroffenen Bereich ein begründeter Verdacht einer Straftaten vorliegt, z. B. Diebstahl, Sachbeschädigung, unbefugten Zugriff auf Datenverarbeitungsanlagen (insbesondere §§ 202 a,303 a, 303 b StGB) oder erhebliche Verschmutzungen hinterlassen wurden.
   b) Der Zeitraum, in dem der Vorfall stattgefunden haben soll, ist näher einzugrenzen. In der Regel sollte er 10 Tage nicht überschreiten. Sollte dies nicht möglich sein, muss der max. Zeitraum mit dem behördlichen Datenschutzbeauftragten abgestimmt werden.
   c) Die Antragstellenden sind die Fachgruppensprecher, die Leiter der Einrichtungen und der AStA. Über den Antrag entscheidet das Rektorat. Die Auswertung (Einsicht ins Zutrittslogbuch) darf nur auf Anordnung des Rektors und mit Zustimmung des Personalrats erfolgen (durch Passwortschutz auch nicht anders möglich, siehe 3.(4)).
   d) Ausdrucke dürfen nur für konkrete Problemstellungen (z.B. Einbruch – bestimmte Türe + Zeitraum) angefertigt werden. Bei internen Ermittlungen ist je Einzelfall zu dokumentieren, wer für welche Zwecke, welche konkreten Daten nutzt (s. Anlage 1). An den Ermittlungen ist der Personalrat zu beteiligen. Ermittlungsbehörden (Staatsanwaltschaft, Polizei, Zoll usw.) können bei konkretem Anlass die Daten anfordern. Der Personalrat und die Zutrittsverwaltung haben dann kurzfristig die Daten zu übermitteln. Dies ist schriftlich zu protokollieren.

8. Zutrittsberechtigungen

(1) Zutrittsberechtigungen können nur auf schriftlichen Antrag an die Zutrittsverwaltung und mit Unterschrift des Dienstvorgesetzten freigeschaltet werden.

(2) Zutrittsberechtigt für Büroräume sind grundsätzlich nur die unmittelbaren Büronutzer sowie deren direkte Dienstvorgesetzte bzw. Raumverantwortliche. Berechtigungen an Dritte sind den Büronutzern mitzuteilen und ausnahmsweise dann möglich, wenn die Büronutzer diesen nicht schriftlich wiedersprechen. Der Wiederspruch ist an den Vorgesetzten zu richten. Findet keine Einigung statt, sind der Rektor und der Personalrat einzubeziehen.

(3) Übergeordnete Zutrittsberechtigungen können nur vom Bereichsleiter (Kanzler, Fachgruppensprecher) für Personen mit besonderen Aufgaben genehmigt werden. Generalzutrittsberechtigungen sind vom Rektorat zu genehmigen. Dem Personalrat ist eine Liste der Personen mit Generalfreischaltung auszuhändigen.

9. Rechte der Personalvertretung

a) Der Personalrat hat das Recht, die Einhaltung dieser Dienstvereinbarung zu überprüfen. Hierzu erhält er auf Verlangen Einsicht in alle mit dem Betrieb des Schließsystems zusammenhängenden Unterlagen, Protokolle und sonstige Aufzeichnungen.

b) Der Personalrat kann vor Ort nach vorheriger Information der Dienststelle Besichtigungen vornehmen.

c) Zur Überprüfung der Arbeitsweise der Anlage im Sinne der Dienstvereinbarung darf der Personalrat Fachleute oder externe Sachverständige zu Rate ziehen.

d)

e) Weitere Beteiligungsrechte der Personalvertretung gem. LPVG Baden- Württemberg bleiben hiervon unberührt.

10. Verhinderung der Leistungskontrolle

Die Staatliche Hochschule für Gestaltung Karlsruhe sichert zu, dass mit Schließsystemen keine Überwachung des Verhaltens und der Leistung der Bediensteten erfolgt.

11. Änderungen, Ergänzungen und Erweiterungen

Änderungen der Dienstvereinbarung können im gegenseitigen Einvernehmen ohne Kündigung der Dienstvereinbarung durchgeführt werden. Hierbei sind die in dieser Dienstvereinbarung bzw. dem LPVG geregelten Rechte der Personalvertretung zu wahren.

12. Schlussbestimmungen

(1) Diese Dienstvereinbarung kann mit einer Frist von drei Monaten zum Jahresende schriftlich gekündigt werden.
(2) Die gekündigte Dienstvereinbarung gilt weiter, bis sich beide Seiten auf eine neue oder auf die Entbehrlichkeit der Dienstvereinbarung oder einzelner Vereinbarungspunkte geeinigt haben.
(3) Kommt binnen sechs Monaten eine Einigung nicht zustande, findet das Stufenverfahren nach § 77 LPVG Anwendung.
(4) Personalrat und Hochschule werden 2 Jahre nach Inkrafttreten aufgrund der gemachten Erfahrungen mit dem Schließsystem über sachlich notwendige Änderungen oder Ergänzungen der Übereinkunft beraten.

13. Inkrafttreten

Diese Dienstvereinbarung tritt mit Ihrer Unterzeichnung in Kraft.

Karlsruhe, _____

Jan Boelen
Rektor

Richard Brunner
Vorsitzender Personalrat

Thomas Fröhlich
Kanzler

Anlage 1
zur Vereinbarung über den Einsatz von elektronischen Schließsystemen

Dienstanweisung für die Sachbearbeiter, die mit elektronischen Schließsystemen arbeiten

1. Allgemeine Hinweise

1.1 Wer das gesetzliche Gebot zur Wahrung des Datengeheimnisses nicht beachtet, verstößt gegen Dienstpflichten oder arbeitsvertragliche Pflichten und handelt u.U. ordnungswidrig oder gar strafbar.

1.2 Die Zuständigkeit des Sachbearbeiters zur Datenverarbeitung/-einsicht beschränkt sich auf die Bereiche und Aufgaben der elektronischen Schließung. Aus den gespeicherten Daten dürfen keine Leistungs-, Verhaltens- oder sonstige Kontrollen erfolgen.

1.3 Neue Sachbearbeiter sind rechtzeitig und umfassend über ihre Aufgabe, die Arbeitsmethode und die Handhabung der Geräte theoretisch und praktisch zu unterrichten. Es ist ausreichend Zeit und Gelegenheit zur Einarbeitung zu geben.

2. Schutzmaßnahmen am Arbeitsplatz gegen unbefugte Zugriffe auf die Datenverarbeitungsanlage (PC) und den Drucker

2.1 Jeder Sachbearbeiter ist für seinen PC und ggf. Drucker datenschutzrechtlich verantwortlich.

2.2 Bei der Arbeit am PC ist ein Bildschirmschoner mit Passwortschutz zu verwenden.

2.3 Passworte sind geheim zu halten und dürfen grundsätzlich nicht an andere Personen weitergegeben werden. Sie dürfen nicht auf dem PC gespeichert werden (auch nicht in Dateien auf Netzlaufwerken), sondern sind an einem sicheren Ort zu verwahren.

2.4 PC-Bildschirm und Drucker sind so aufzustellen, dass Unbefugte weder den Bildschirminhalt noch die Druckausgabe einsehen können.

2.5 Sämtliche personenbezogenen Daten sind so zu verwahren, dass kein Unbefugter Zutritt erlangen kann.

3. Behandlung von personenbezogenen Daten in Auswertungen

3.1 Dokumente und Auswertungen mit personenbezogenen Daten in Papierform sind nach Dienstgebrauch mit dem Reißwolf in der zu diesem Zeitpunkt gültigen DIN zu vernichten.

3.2 Bei Dienstende sind Dokumente und Listen mit personenbezogenen Daten einzuschließen.

3.3 Personenbezogene Daten oder Dokumente und Auswertungen mit personenbezogenen Daten dürfen mittels Netzdiensten (Elektronische Post - z.B. E-Mail) nur passwortgeschützt versandt werden.

3.4 Die Weitergabe von Auswertungen von Daten (Listen etc.) an Externe ist nur an Ermittlungsbehörden zulässig, wenn diese angefordert werden.

3.5 Auswertungen auf Papierform (Listen etc.) sind mit dem Aufdruck „Datenschutzsache. Nach Dienstgebrauch nur per Reißwolf vernichten" zu versehen.

3.6 Die Dokumentation bei Auswertungen gemäß § 7 dieser Dienstvereinbarung ist mittels Formular

auf dem Netzlaufwerk, „Zutrittsverwaltung" zu erstellen und dort zu speichern.

Anlage 2

zur Vereinbarung über den Einsatz von elektronischen Schließsystemen

Bedienungsanleitung für das elektronische Schließsystem ENIQ DOM Zutrittskontrolle

Bedienungshinweise

a) Der neue Hochschulausweis wird zeitgleich eingeführt. Die Karte muss einmal freigeschaltet werden. Dieses Gerät befindet sich bei einem Administrator.
b) Die Karte muss mit Rechten versehen werden. Dies geschieht an „Update-Terminals". Einmal und danach nur bei Änderungen in ihren Berechtigungen - was in der Regel nur bei Umzug, neuer Raumzuordnung oder Versetzung vorkommen wird.
   Dieses Gerät befindet sich am Haupteingang Lorenzstr. 15.
c) Die Gültigkeit der Karte muss (i.d.R.) in einer definierten Zeit bestätigt werden. Dies geschieht am Update-Terminal. Es entstehen also hierdurch keine zusätzlichen Wege. Durch diese monatliche Validierung für die Innentüren und eine halbjährliche Validierung für die Außentüren kann die Karte bei Verlust gesperrt werden, indem der Besitzer eine Verlustmeldung an eine zentrale Meldestelle bzw. einer E-Mail-Adresse die auf der Homepage bekannt gegeben wird gibt. Auch die Offline-Komponenten erkennen die fehlende Validierung, welche bei Sperrung der Karte natürlich versagt wird.

Anleitung für Türschlösser

Die Anleitung und die Bedeutung der Bediensignale ist beigefügt und auf der Homepage abrufbar.

Anlage 3

zur Vereinbarung über den Einsatz von elektronischen Schließsystemen

Personaldaten aus Personalverwaltung und Studierendenverwaltung

In das ENIQ DOM Eintrittskontrolle werden Daten übernommen:

- aus der Personalverwaltung mit der aktuellen Software
- aus der Studierendenverwaltung mit der aktuellen Software

Gespeichert werden nur Name, Vorname und Kartennummer.

Anlage 4

zur Vereinbarung über den Einsatz von elektronischen Schließsystemen

Rollenkonzept

Der Datenzugriff ist nur mit der Zustimmung der Dienststellenleitung und des Personalrates zulässig.