Amtliche Bekanntmachungen
der Pädagogischen Hochschule Freiburg

2018, Nr. 24 27. Juni 2018

Satzung der Pädagogischen Hochschule Freiburg über den Einsatz von elektronischen Zugangskontrollsystemen

vom 25. Juni 2018

Aufgrund von § 12 Abs. 4 des Landeshochschulgesetzes (LHG) vom 1. Januar 2005 (GBl. S. 1), in der Fassung vom 13. März 2018 (GBl, S. 85) hat der Senat der Pädagogischen Hochschule Freiburg gemäß § 19 Abs. 1 Satz 10 LHG am 13. Juni 2018 die folgende Satzung beschlossen:

§ 1 Gegenstand und Zielsetzung

Die Pädagogische Hochschule betreibt ein elektronisches Zugangskontrollsystem zur Gewährleistung der Sicherheit für Personal und Gegenstände in den Gebäuden und zur effizienteren und wirtschaftlicheren Verwaltung der Zutrittsberechtigungen. Die personenbezogenen Daten werden ausschließlich zu dem im Satz 1 genannten Zweck verarbeitet, die Verarbeitung zu anderen Zwecken, insbesondere zur Überwachung des Verhaltens und der Leistungen der Beschäftigten der Hochschule ist ausgeschlossen.
Diese Satzung regelt die Ausgestaltung, den Einsatzzweck und den Betriebsablauf des elektronischen Zugriffskontrollsystems.

§ 2 Geltungsbereich

(1) Der räumliche Geltungsbereich umfasst alle von der Pädagogischen Hochschule genutzten Gebäude und Außenflächen.

(2) Die Bestimmungen gelten für alle Mitglieder und Angehörigen der Pädagogischen Hochschule.

§ 3 Datenerfassung

(1) Die Datenerfassung erfolgt mit dem netzwerkfähigen elektronischen Schließsystem SALTO ProAccess Space, welches die Personendaten aus dem Identitätsmanagement der

Hochschule über eine Zwischentabelle erhält und diese mit den für die Schließung notwendigen Daten in einer Datenbank vorhält.

In dieser Datenbank werden folgende Angaben bereitgestellt:

- Die eindeutige Identitätsnummer aus dem IDM-System
- Transponderbesitzer/in mit Vor- und Nachnamen
- Titel
- Personen-Aktivierungsdatum
- Personen-Ablaufdatum
- Schließberechtigung für Gebäude und Räume

In den digitalen Zylindern bzw. Beschlägen können bauartbedingt bis zu 1000 verschlüsselte Ereignisse mit den Daten:

- Transponder ID
- Datum
- Uhrzeit

gespeichert werden.

Die Initialisierung der Zylinder und Beschläge, sowie das Auslesen der Daten an Zylindern und Beschlägen kann nur mit einem systemkonfigurierten und für die Software zugelassenen Programmiergerät an jeder Tür erfolgen. Die abgegriffenen Daten müssen danach vom Programmiergerät über die Software übertragen werden und können nur dort von den berechtigten Personen ausgelesen werden.

Für alle Ereignisse, die über die Wandleser und Onlinetüren in der Datenbank der Saltosoftware gespeichert werden, erfolgt täglich die Übertragung in eine Bereinigungsdatei. Die Daten werden jeweils nach 14 Tagen nach der Übertragung auf den Server gelöscht.

Von hochschulfremden Personen, die ein Medium erhalten, werden keine personenbezogenen Daten erfasst.

(2) Schließversuche mit unberechtigtem Transponder werden ebenfalls gespeichert.

(3) In den Transpondern werden neben der Transpondernummer und Transponder-ID die Räume mit Raumnummer, Datum und Uhrzeit gespeichert, die mit diesem Transponder geöffnet bzw. verschlossen wurden. Mit Erreichen der Speicherkapazität von 50 Ereignissen werden keine weiteren Daten gespeichert, bis das Medium an einem Updateleser ausgelesen wird. Der Updateleser überträgt die Daten auf den Server und wird gleichzeitig geleert. Die Daten sind gegen unbefugtes Auslesen mittels Software durch ein Passwort nach § 4 geschützt.

§ 4 Regelung der Einsichtnahme

(1) Eine Nutzung der gespeicherten Daten erfolgt nur bei (a.) Vorfällen von strafrechtlicher Relevanz, bei (b.) gravierenden sicherheitsrelevanten Ereignissen und (c.) bei einem hinreichenden Verdacht gröblicher Dienstpflichtsverletzungen[i].

(2) Eine Weitergabe der Daten erfolgt bei strafrechtlich relevanten Ereignissen an die zuständigen Ermittlungsbehörden und sonst nur im Einvernehmen mit dem Datenschutzbeauftragten der Hochschule. Sofern eine Auswertung der Daten durch die Pädagogische Hochschule erforderlich ist, erfolgt die Einsichtnahme in die gespeicherten Daten auf Anordnung der Kanzlerin/des Kanzlers im Vier-Augen-Prinzip durch die/den zuständigen Administrator/in, unter Hinzuziehung eines/r Vertreters/in des Personalrates. Der Datenschutzbeauftragte wird informiert.

(3) Die nach der Übertragung auf dem Server gespeicherten Zugangsdaten werden für zwei Wochen gespeichert und dann gelöscht. Diese Speicherdauer ist notwendig, da in der vorlesungsfreien Zeit z.B. Diebstähle erfahrungsgemäß erst mit Verzögerung auffallen. Die Stammdaten bleiben ein Jahr gespeichert, denn Lehrbeauftragte setzen häufig für ein Semester aus.

(4) Soweit dies für die Konfiguration, die Funktionsprüfung der Türen sowie die Behebung von technischen Mängeln oder Bedienungsfehlern erforderlich ist, erhalten die Mitarbeiter/innen des Technischen Dienstes Zugriff zum System, davon ausgeschlossen ist der Zugriff auf Ereignisdaten von Schließvorgängen. Die/der Adminstrator des ZIK schaltet die Berechtigungen entsprechend frei.

§ 5 Pflichten der Nutzer

(1) Die/der Nutzer hat den Transponder mit der gebotenen Sorgfalt zu verwahren.

(2) Die/der Nutzer ist verpflichtet, bei Verlust oder Beschädigung des Transponders dessen Sperrung beim Technischen Dienst unverzüglich zu veranlassen.

§ 6 Inkrafttreten

Diese Ordnung tritt am Tag nach ihrer Veröffentlichung in Kraft.

Freiburg, den 25. Juni 2018

gez. Druwe

Prof. Dr. Ulrich Druwe
Rektor

---

[i] Der Personalrat hat mit Schreiben vom 21. Juni 2018 gemäß § 75 Abs. 4 Nr. 11, Alternative 2 Landespersonalvertretungsgesetz (LPersVG) der Verfahrensweise gemäß § 4 Abs. 1 c in Verbindung mit Abs. 2 Satz 2 f der Satzung der Pädagogischen Hochschule Freiburg über den Einsatz von elektronischen Zugangskontrollsystemen zugestimmt.