Allgemeine Beschreibung der eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen nach Art. 7 und 8 BayDSG

(**X**) Erstmalige Beschreibung
( ) Änderung der Beschreibung vom

1. Allgemeine Angaben

Bezeichnung des Verfahrens	Stand dieser Beschreibung
Elektronische Schließanlage	06.10.2014
Nähere Auskünfte erteilt	Telefon
N.N. (Administrator)	09071 53-XXX

2. Eingesetzte Datenverarbeitungsanlagen und Programme

Bezeichnung (z. B. Server im PC-Netzwerk, Intranet oder Internet bzw. Einzelplatzrechner) und Standort der Anlage
Server: SQL-Server Intra-db01 1 virtueller PC als Hauptstation: intra-zutritt (beide im Serverraum der ALP) 2 Notzebooks und 1 PC in der Rezeption 1 PC (Hausmeister) 1 PC (Administrator) Alle Geräte befinden sich im Intranet der ALP.
Eingesetzte(s) Betriebssystem(e)
Windows 2008 Server, SQL 2008, Windows 7
Eingesetzte Software (z. B. Standardsoftware, Datenbanken, spezielle für das freizugebende Verfahren erworbene oder selbst erstellte Software)
Salto Hams RW Pro-Access von SALTO Systems GmbH Deutschland Gewerbestr. 5 58285 Gevelsberg

3. Maßnahmen zur Sicherstellung der jederzeitigen Verfügbarkeit der gespeicherten Daten

(z. B. Anfertigung von Sicherheitskopien, Maßnahmen zur Virenbekämpfung, Wiederanlaufverfahren, Notfallkonzept)

Tägliche Datenbank-Sicherung (zusammen mit allen anderen Datenbanken der ALP)
Mehrstufiger Viren und Hacking-Schutz, identisch für alle Anlagen der ALP: Kontrolle bzw. Sperrung von Ports, stets aktuelle Anti-Viren und Anti-Spy-Software sowohl auf den Servern wie auf allen Endgeräten.
Da die Zugangskontrolle offline erfolgt und alle Türschlösser mit Batterien ausgestattet sind, sind keine speziellen Maßnahmen zum Wiederanfahren nötig.
Alle Türen können mit einem Spezialschlüssel bzw. einem Generalschlüssel geöffnet werden (nur für Berechtigte in je einem versperrten Schlüsselkasten an der Rezeption bzw. im Büro XXX).

4. Weitere technische und organisatorische Maßnahmen nach Art. 7 und 8 BayDSG

(z.B. Schutzmaßnahmen für den Rechnerraum; Maßnahmen zur sicheren Aufbewahrung der Datenträger; Festlegung und Dokumentation der zum Lesen, zur Eingabe oder zur Übermittlung berechtigter Personen; Zugriffskontrolle mittels Passwort; Protokollierung von Eingaben; Erstellung von Richtlinien und Arbeitsanweisungen; Absicherung gegen unbefugten Zugriff Dritter; Sicherung der Vertraulichkeit beim Transport oder der Übermittlung von Daten)

Der Rechnerraum ist durch ein Zahlenschloss und ein Transponderschloss gesichert.

Datenträger der Datensicherung werden zusammen mit denen aller übrigen Systeme in einem gesonderten, abgesicherten Raum aufbewahrt.

Administrator mit allen Zugriffsrechten ist N. N.
Wartungsmitarbeiter (stellvertretender Administrator): N. N.

Der Zugang zur Systemadministration und zur Wartung ist passwortgesichert sowie an die oben genannten Endgeräte gebunden.

Alle Eingaben ins System werden von diesem mitprotokolliert, ebenso alle Aktivitäten der Schlüsselkarten bzw. Tokens an den Türen. Der Zugang zu diesen Daten ist nur dem Administrator und seinem Stellvertreter möglich. Die Daten sind passwortgeschützt.

Die Schließaktionen werden auf einem Memorychip in den jeweiligen Türschlössern gespeichert. Sie können nur mit einem Spezial-Lesegerät von Salto-Systems ausgelesen werden.
Bei Gästen beinhaltet die Schließkarte keinen Namen, lediglich die Zimmernummer. Die Daten der Gästekarte werden am Ende des Berechtigungszeitraums gelöscht (in der Regel am letzten Lehrgangstag). Sie können dann nur noch aus den

Türspeichern rekonstruiert werden.

Es gibt einige wenige „Online“-Zugänge, an denen die Mitarbeiter-Tokens täglich einmal freigeschaltet werden müssen. Dies sind:

- Haupteingang der ALP (Glastür)
- Seiteneingang Kardinal-von-Waldburg-Str. (Gittertür)
- KFZ-Einfahrt Konviktstraße
- Tor zum Küchenhof, Klosterstr. 1

Die Aktivitäten an diesen Zugangspunkten können vom Sysadmin unmittelbar ausgelesen werden. Die Namen der Tokeninhaber werden in Klartext angezeigt.

Aktivitäten an den Türen der Gästesimmer, der Büros, der Hörsäle und allen anderen Räumen werden in den Schlössern gespeichert und können nur mit einem Spezialscanner der Firma SALTO ausgelesen werden.
Die Gäste-Identität ist dabei nicht unmittelbar feststellbar, sie kann über das Zimmerverwaltungssystem anhand der Zimmernummer aber rekonstruiert werden.
Die Identität der Mitarbeiter ist unmittelbar ersichtlich.

Das Auslesen von personenbezogenen Daten ist nur nach Anweisung durch die Direktion und im 4-Augen-Prinzip gestattet (siehe Dienstvereinbarung „Schließanlage“).

Datum	Unterschrift
Dillingen, Datum	Datenschutzbeauftragter