

# **Technische und organisatorische Maßnahmen**

**Technische und organisatorische Maßnahmen für  
den Housing-Betrieb SIGUV-Rechenzentrum**



# Technische und organisatorische Maßnahmen

2

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

### 1.1. Zutrittskontrolle

Verwaltung:

- Alarmanlage
- Chipkarten / Transpondersysteme
- Manuelles Schließsystem
- Sicherheitsschlösser
- Schließsystem mit Codesperre
- Videoüberwachung und Sensorische Überwachung
- Empfang / Rezeption / Wachpersonal
- Besucherregistrierung und Ausweisausgabe
- Besucher in Begleitung des HDP-Personals
- Sorgfältige Auswahl des Wachpersonals

Rechenzentrum:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um das gesamte Rechenzentrum
- dokumentierte Schlüsselvergabe
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Sicherheitszentrale zur Überwachung des Betriebs-geländes und des Rechenzentrums
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Firmen) zu den Räumen des RZ ist wie folgt beschränkt: Nur in Begleitung einer Zutrittsberechtigten Person.

### 1.2. Zugangskontrolle

Durch den Einsatz von sorgfältig ausgewähltem Wachpersonal und eines Zutrittskontrollsystems wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt bzw. beschädigt werden können.

# Technische und organisatorische Maßnahmen

3

## 1.3. Zugriffskontrolle

Für den Zugriff auf Datenträger von Kunden (Housing-Nehmern) ist ausschließlich das Team DCIM im Rahmen von Service Request autorisiert.

Der Zugriff erfolgt in Einzelfällen im Rahmen von Datensicherungsaktivitäten auf spezifische Datenträger. Diese Aktivität erfolgt auf explizite Anweisung und Überwachung der Kunden.

Die Verantwortlichkeiten in Bezug auf Informations- und Cybersicherheit für das SIGUV-Rechenzentrum sind getrennt organisiert.

- Über das Corporate Network der Unfallversicherungsträger (CNUV) versorgt die IT der Deutschen Gesetzlichen Unfallversicherung (DGUV) die Träger der gesetzlichen Unfallversicherung deutschlandweit mit einem gemeinsamen abgesicherten Datennetz.
- Getrennt vom Netzwerk der Server sind die Systeme der Rechenzentrum-Infrastruktur vor unerlaubtem Zugriff geschützt. Dieses liegt in der Verantwortung der IT der HDP GmbH.

## 1.4. Trennungskontrolle

Ist im Rahmen des Housing-Betriebes nicht geschäftliche Praxis.

## 2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

### 2.1. Weitergabekontrolle

Ist im Rahmen des Housing-Betriebes nicht geschäftliche Praxis.

### 2.2. Eingabekontrolle

Ist im Rahmen des Housing-Betriebes nicht geschäftliche Praxis.

### 2.3. Auftragskontrolle

Ist im Rahmen des Housing-Betriebes nicht geschäftliche Praxis.

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

### 3.1. Verfügbarkeitskontrolle

Unterbrechungsfreie Stromversorgung, Überwachung von Temperatur und Feuchtigkeit in den Serverräumen, Klimaanlage in den Serverräumen, Schutzsteckdosenleisten in den Serverräumen, Feuerlöscheinrichtungen in den Serverräumen, Feuer- und Rauchmeldeanlage.

### 3.2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Eine rasche Wiederherstellung der Verfügbarkeit wird mittels der Prozeduren des Notfallhandbuch SIGUV-Rechenzentrum gelenkt.