1. **Zutrittskontrolle:**

Zweck der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verhindern.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  | Alarmanlage |  | | Personenkontrolle beim Empfang |
|  | Absicherung von Gebäudeschächten |  | | Protokollierung Besucher |
|  | autom. Zugangskontrollsystem |  | | Schlüsselregelung |
|  | Chipkarten-/Transponder-Schließsystem |  | | Sorgfältige Auswahl von Sicherheitspersonal |
|  | Bewegungsmelder |  | | Tragepflicht von Mitarbeiter-/Gästeausweis |
|  | Manuelles Schließsystem |  | | Videoüberwachung der Zugänge |
|  | Schließsystem mit Codesperre |  | |  |
|  | Sicherheitsschlösser |  | |  |
|  | Verschlossener Serverraum/-schrank |  | |  |

1. **Zugangskontrolle:**

Durch Maßnahmen der Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  | Authentifikation mit Benutzer & Passwort |  | | Verwaltung Benutzerberechtigungen |
|  | Einsatz von Anti-Viren-Software |  | | Erstellen von Benutzerprofilen |
|  | Einsatz einer Firewall |  | | Passwortvergabe/Passwortregeln |
|  | Einsatz von Mobile Device Management |  | | Bildschirm für Unbefugte nicht einsehbar aufstellen |
|  | Einsatz von VPN-Technologie |  | |  |
|  | Sperren externer Schnittstellen |  | |  |
|  | Verschlüsselung von Datenträgern |  | |  |
|  | Verschlüsselung von Smartphones |  | |  |
|  | Sperren Bildschirm |  | |  |

1. **Zugriffskontrolle:**

Die Zugriffskontrolle soll sicher stellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten nur Zugriff auf die ihrer Zugriffsberechtigung entsprechenden Daten haben und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  | Einsatz von Aktenvernichtern |  | | Begrenzung administrativer Rechte auf notwendigsten Personenanzahl |
|  | Ordnungsgemäße Vernichtung von Daten (DIN32757) |  | | Einsatz von zertifizierten Dienstleistern zur Datenvernichtung |
|  | Vernichtung der Daten auf Datenträgern vor deren Weitergabe |  | | Erstellen eines Berechtigungskonzepts |
|  | Protokollierung der Datenvernichtung |  | | Passwortrichtlinie inkl. Länge und Lebensdauer |
|  | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten |  | | Sichere Aufbewahrung von Datenträgern |

1. **Weitergabekontrolle:**

Bei der Weitergabekontrolle soll sichergestellt werden, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt ist.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  | Einrichtung von VPN-Tunneln |  | | Dokumentation der Datenempfänger sowie der Zeitspannen der geplanten Überlassung bzw. vereinbarte Löschfristen |
|  | Verschlüsselung E-Mails |  | | Erstellen einer Übersicht aller regelmäßigen Abruf- und Übermittlungsvorgängen |
|  | Sichere Transportbehälter |  | | Sorgfältige Auswahl von Transportpersonal und –fahrzeugen |
|  |  |  | | Weitergabe von personenbezogenen Daten anonymisiert oder pseudonymisiert (Schlüssel darf nicht gleichzeitig übermittelt werden) |

1. **Eingabekontrolle:**

Diese Maßnahmen sollen sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  | Protokollierung der Eingabe, Änderung und Löschung von Daten |  | | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
|  |  |  | | Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, verändert oder gelöscht werden können |
|  |  |  | | Nachvollziebarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (keine Benutzergruppen) |
|  |  |  | | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |

1. **Auftragskontrolle:**

Die Auftragskontrolle bezieht sich auf die Verarbeitung personenbezogener Daten bei einem Auftragsverarbeiter. Dabei muss gewährleistet sein, dass personenbezogenen Daten, die im Auftrag weiter verarbeitet werden, ausschließlich entsprechend den Weisungen des Auftraggebers verarbeitet werden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  |  |  | | Sorgfältige Auswahl des Auftragsverarbeiters |
|  |  |  | | Laufende Überprüfung des Auftragnehmers |
|  |  |  | | Vertrag zwischen Auftraggeber und Auftragnehmer incl. Vertragsstrafen, Verschwiegenheitspflicht Mitarbeiter, getroffener Sicherheitsmaßnahmen, Kontrollrechte des Auftraggebers gegenüber Auftragsnehmer |

1. **Verfügbarkeitskontrolle:**

Die Verfügbarkeitskontrolle soll sicherstellen, dass personenbezogenen Daten gegen Zerstörung und Verlust geschützt sind.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  | Feuerlöscher im Serverraum/Rechenzentrum |  | | Alarm bei unberechtigten Zutritten zu Serverraum/Rechenzentrum |
|  | Feuer- und Rauchmelder im Rechenzentrum/Serverraum |  | | Aufbewahrung von Datensicherungen an einem sicheren Ort z.B. feuerfester Tresor, im besten Fall an einem ausgelagerten Ort |
|  | Klimatisierung von Serverraum/Rechenzentrum |  | | Erstellen eines Backup- und Recovery-Konzepts |
|  | USV |  | | Schutz der Serverräume vor Überflutungen |
|  | Überwachung von Feuchtigkeit und Temperatur im Serverraum/Rechenzentrum |  | | Erstellen eines Notfallplans |

1. **Trennungsgebot:**

Mit dem Trennungsgebot soll gewährleistet werden, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden und keine Durchmischung erfolgt.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technische Maßnahmen** | | | **Organisatorische Maßnahmen** | |
|  | Bei pseudonymisierten Daten Trennung des Schlüssels von den eigentlichen Datensätzen |  | | Erstellung Berechtigungskonzept |
|  | Physikalisch getrennte Speicherung auf gesonderten Systemen und Datenträgern |  | | Festlegung von Datenbankrechten |
|  | Trennung Produktiv- und Testsystem |  | | Softwareseitige Mandantentrennung |
|  |  |  | | Versehen der Datensätze mit Zweckhinweisen |