# Anlage 1 – Sicherheit der Verarbeitung

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

|  |  |  |  |
| --- | --- | --- | --- |
| Zutrittskontrolle | | | |
|  | Alarmanlage |  | Absicherung von Gebäudeschächten |
|  | Automatisches Zugangskontrollsystem |  | Chipkarten-/Transponder-Schließsystem |
|  | Schließsystem mit Codesperre |  | Manuelles Schließsystem |
|  | Biometrische Zugangssperren |  | Videoüberwachung der Zugänge |
|  | Lichtschranken / Bewegungsmelder |  | Sicherheitsschlösser |
|  | Schlüsselregelung (Schlüsselausgabe etc.) |  | Personenkontrolle beim Pförtner / Empfang |
|  | Protokollierung der Besucher |  | Sorgfältige Auswahl von Reinigungspersonal |
|  | Sorgfältige Auswahl von Wachpersonal |  | Tragepflicht von Berechtigungsausweisen |
| Anmerkungen / Details | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Zugangskontrolle | | | |
|  | Zuordnung von Benutzerrechten |  | Erstellen von Benutzerprofilen |
|  | Passwortvergabe |  | Authentifikation mit biometrischen Verfahren |
|  | Authentifikation mit Benutzername / Passwort |  | Zuordnung von Benutzerprofilen zu IT-Systemen |
|  | Gehäuseverriegelungen |  | Einsatz von VPN-Technologie |
|  | Sperren von externen Schnittstellen (USB) |  | Einsatz einer Software-Firewall |
|  | Verschlüsselung von Datenträgern in Laptops / Notebooks |  | Einsatz einer Hardware-Firewall |
|  | Einsatz von Anti-Viren-Software |  | Verschlüsselung von Smartphone Inhalten |
|  | Einsatz von Intrustion-Detection-Systemen |  | Verschlüsselung von mobilen Datenträgern |
|  | Einsatz einer Spyware & PUAs Software |  | Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |
|  | Zuordnung von Benutzerrechten |  | Erstellen von Benutzerprofilen |
| Anmerkungen / Details | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Zugriffskontrolle | | | |
|  | Erstellen eines Berechtigungskonzepts |  | Verwaltung der Rechte durch Systemadministrator |
|  | Anzahl der Administratoren auf das „Notwendigste“ reduziert |  | Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
|  | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten |  | Sichere Aufbewahrung von Datenträgern |
|  | physische Löschung von Datenträgern vor Wiederverwendung |  | ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
|  | Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) |  | Protokollierung der Vernichtung |
|  | Verschlüsselung von Datenträgern |  | Angemessene Datenschredder |
| Anmerkungen / Details | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Trennungskontrolle | | | |
|  | physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern |  | Logische Mandantentrennung (softwareseitig) |
|  | Erstellung eines Berechtigungskonzepts |  | Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
|  | Versehen der Datensätze mit Zweckattributen/Datenfeldern |  | Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
|  | Festlegung von Datenbankrechten |  | Trennung von Produktiv- und Testsystem |
| Anmerkungen / Details | | | |
|  | | | |

|  |  |
| --- | --- |
| Pseudonymisierung | |
|  | Weitergabe von Daten in pseudonymisierter Form |
| Anmerkungen / Details | |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| Eingabekontrolle | | | |
|  | Protokollierung der Eingabe, Änderung und Löschung von Daten |  | Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
|  | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |  | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
|  | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |  | Sonstiges: |
| Anmerkungen / Details | | | |
|  | | | |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Weitergabekontrolle | | | |
|  | Einrichtungen von Standleitungen bzw. VPN-Tunneln |  | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
|  | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen |  | Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen |
|  | E-Mail Verschlüsselung |  | Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| Anmerkungen / Details | | | |
|  | | | |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Verfügbarkeitskontrolle | | | |
|  | Unterbrechungsfreie Stromversorgung (USV) |  | Klimaanlage in Serverräumen |
|  | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen |  | Schutzsteckdosenleisten in Serverräumen |
|  | Feuer- und Rauchmeldeanlagen |  | Feuerlöschgeräte in Serverräumen |
|  | Alarmmeldung bei unberechtigten Zutritten zu Serverräumen |  | Erstellen eines Backup- & Recoverykonzepts |
|  | Testen von Datenwiederherstellung |  | Erstellen eines Notfallplans |
|  | Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort |  | Serverräume nicht unter sanitären Anlagen |
|  | In Hochwassergebieten: Serverräume über der Wassergrenze |  | Durchführung von Penettrationstests |
| Anmerkungen / Details | | | |
|  | | | |

# Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

|  |  |  |  |
| --- | --- | --- | --- |
| Datenschutzmanagement | | | |
|  | Vorfallreaktionsplan ist vorhanden (Incident-Response-Management) |  | Datenschutzmanagementsystem vorhanden |
| Anmerkungen / Details | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) | | | |
|  | Privacy by default eingehalten |  | Privacy bei Design eingehalten |
| Anmerkungen / Details | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Auftragskontrolle (Art. 28 DS-GVO) | | | |
|  | Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) |  | vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
|  | schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)  i.S.d. **Art. 28 ff. EU-DSGVO** |  | Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis |
|  | Auftragnehmer hat Datenschutzbeauftragten bestellt |  | Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
|  | Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart |  | laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |
|  | Vertragsstrafen bei Verstößen |  | Sonstiges: |
| Anmerkungen / Details | | | |
|  | | | |

|  |
| --- |
| Schlussbemerkung |
|  |

|  |  |  |
| --- | --- | --- |
| Ort, Datum: | Unterschrift Gesprächspartner: | Unterschrift WENZA Betreuer: |
|  |  |  |

