***Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO***

Anlage 1 zur Prüfung des AVV der

Name und Anschrift des Unternehmens, mit dem der AVV geschlossen wird

Prüfdatum:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Regelungen zur Vertraulichkeit (Nr. 9 der Checkliste)** | | | |
|  | | | |
| 1. **Zutrittskontrolle - Technische Maßnahmen** | | **Zutrittskontrolle - Organisatorische Maßnahmen** | |
| Hierbei handelt es sich um Maßnahmen, die geeignet sind, den Zutritt Unbefugter zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verhindern. | | | |
| Alarmanlage |  | Schlüsselregelung/-listen |  |
| Automatisches Zugangskontrollsystem |  | Empfang/Rezeption/Pförtner |  |
| Biometrische Zugangssperren |  | Besucherbuch/Protokoll der Besucher |  |
| Chipkarten/Transpondersystem |  | Mitarbeiter-/Besucherausweise |  |
| Manuelles Schließsystem |  | Besucher in Begleitung durch Mitarbeiter |  |
| Sicherheitsschlösser |  | Sorgfalt bei Auswahl des Wachpersonals |  |
| Schließsystem mit Codesperren |  | Sorgfalt bei Auswahl des Reinigungsdienstes |  |
| Absicherung der Gebäudeschächte |  |  |  |
| Türen mit Knauf Außenseiten |  |  |  |
| Klingelanlage mit Kamera |  |  |  |
| Videoüberwachung der Eingänge |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **b) Zugangskontrolle - Technische Maßnahmen** | | **Zugangskontrolle - Organisatorische Maßnahmen** | |
| Maßnahmen, die geeignet sind, Unbefugte an der Nutzung der Datenverarbeitungssysteme zu hindern. | | | |
| Login mit Benutzername und Passwort |  | Verwaltung von Benutzerberechtigungen (periodische Überprüfung) |  |
| Login mit biometrischen Daten |  | Erstellen von Benutzerprofilen |  |
| Anti-Viren-Software Server |  | Zentrale Passwortvergabe |  |
| Anti-Viren-Software Clients |  | Richtlinie für sichere Passwörter (Mindestlänge, Komplexität, Wechsel erzwungen) |  |
| Anti-Viren-Software mobile Geräte |  | Richtlinie zum Löschen und Vernichten |  |
| Firewall |  | Richtlinie für Clean desk |  |
| Intrusion Detection Systeme |  | allg. Richtlinie für Datenschutz und/oder Sicherheit |  |
| Mobile Device Management |  | Mobile Device Policy |  |
| Einsatz VPN bei Remote-Zugriff |  |  |  |
| Verschlüsselung von Datenträgern |  |  |  |
| Verschlüsselung von Smartphones |  |  |  |
| Gehäuseverriegelung |  |  |  |
| BIOS-Schutz |  |  |  |
| Sperre externer Schnittstellen (USB) |  |  |  |
| Automatische Desktopsperre |  |  |  |
| Verschlüsselung von Notebooks/Tablets |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **c) Zugriffskontrolle - Technische Maßnahmen** | | **Zugriffskontrolle - Organisatorische Maßnahmen** | |
| Hierbei handelt es sich um Maßnahmen, dass ausschließlich berechtigte Personen ein Datenverarbeitungssystem nutzen und nur auf die ihrer Berechtigung unterliegenden Daten zugreifen können. Zudem gewährleisten diese Maßnahmen, dass die Daten nach der Speicherung nicht unbefugterweise gelesen, kopiert, verändert oder gelöscht werden können. | | | |
| Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten |  | Rechte-/Rollenkonzept |  |
| Physische Vernichtung von Datenträgern |  | möglichst minimale Anzahl an Administratoren |  |
|  |  | Datenschutztresor |  |
|  |  | Verwaltung der Benutzerrechte durch Administratoren |  |
|  |  |  |  |
|  |  |  |  |
| **d) Trennungskontrolle - Technische Maßnahmen** | | **Trennungskontrolle - Organisatorische Maßnahmen** | |
| Mit diesen Maßnahmen gewährleistet der Auftragsverarbeiter, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet werden können. | | | |
| Trennung von Produktiv- und Testumgebung |  | Steuerung über Berechtigungskonzept |  |
| Physikalische Trennung (Systeme/Datenbanken/Datenträger) |  | Festlegung von Datenbankrechten |  |
| Mandantenfähigkeit relevanter Anwendungen |  | Datensätze sind mit Zweckattributen versehen |  |
|  |  |  |  |
|  |  |  |  |
| **e) Pseudonymisierung - Technische Maßnahmen** | | **Pseudonymisierung - Organisatorische Maßnahmen** | |
| Die personenbezogenen Daten werden so verarbeitet, dass eine Zuordnung zu einer spezifischen Person nur noch mit Hilfe zusätzlicher Informationen möglich ist, sofern diese gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. | | | |
| Trennung der Zuordnungsdaten und Aufbewahrungsdaten in getrennten und abgesicherten System |  | interne Anweisung, dass die Daten im Falle der Weitergabe oder nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren sind |  |
| Aufbewahrung möglichst verschlüsselt |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **2. Regelungen zur Integrität (Nr. 10 der Checkliste)** | | | |
|  |  |  |  |
| 1. **Weitergabekontrolle - Technische Maßnahmen** | | **Weitergabekontrolle - Organisatorische Maßnahmen** | |
| Mit Hilfe dieser Maßnahmen wird sichergestellt, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht durch unbefugte gelesen, kopiert, verändert oder entfernt werden können. Zudem kann dadurch überprüft und festgestellt werden, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist. | | | |
| E-Mail-Verschlüsselung (S/MIMI/PGP) |  | Dokumentation der Datenempfänger sowie Dauer der geplanten Überlassung bzw. der Löschfristen |  |
| E-Mail-Signatur (S/MIME/PGP) |  | Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge |  |
| Einsatz von VPN |  | Weitergabe in anonymisierter oder pseudonymisierter Form |  |
| Protokollierung der Zugriffe und Abrufe |  | Sorgfalt bei der Auswahl von Transport-Personal und Fahrzeugen |  |
| Sichere Transportbehälter |  | Persönliche Übergabe mit Protokoll |  |
| Bereitstellung über verschlüsselte Verbindungen wie sftp, https |  |  |  |
| Nutzung von Signaturverfahren |  |  |  |
|  |  |  |  |
| **b) Eingabekontrolle - Technische Maßnahmen** | | **Eingabekontrolle - Organisatorische Maßnahmen** | |
| Durch diese Maßnahmen wird gewährleistet, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogenen Daten ins DV eingegeben, verändert oder entfernt worden sind. | | | |
| Technische Protokollierung der Eingabe, Änderung und Löschung von Daten |  | Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können |  |
| Manuelle oder automatisierte Kontrolle der Protokolle |  | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |  |
|  |  | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |  |
|  |  | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden |  |
|  |  | Klare Zuständigkeiten für Löschungen |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **3. Regelungen zur Verfügbarkeit und Belastbarkeit (Nr. 11 und Nr. 12 der Checkliste)** | | | |
|  |  |  |  |
| **Verfügbarkeitskontrolle - Technische Maßnahmen** | | **Verfügbarkeitskontrolle - Organisatorische Maßnahmen** | |
| Feuer- und Rauchmeldeanlagen |  | Backup & Recovery-Konzept (ausformuliert) |  |
| Feuerlöscher Serverraum |  | Kontrolle des Sicherungsvorgangs |  |
| Serverraumüberwachung Temperatur und Feuchtigkeit |  | Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |  |
| Serverraum klimatisiert |  | Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums |  |
| USV |  | Keine sanitären Anschlüsse im oder oberhalb des Serverraums |  |
| Schutzsteckdosenleisten Serverraum |  | Existenz eines Notfallplans (z.B. BSI IT Grundschutz 100-4) |  |
| Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.) |  | Getrennte Partitionen für Betriebssysteme und Daten |  |
| RAID System/Festplattenspiegelung |  |  |  |
| Videoüberwachung Serverraum |  |  |  |
| Alarmmeldung bei unberechtigtem Zutritt zu Serverraum |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Nr. 13 der Checkliste)** | | | |
|  |  |  |  |
| 1. **Datenschutz-Management - Technische Maßnahmen** | | **Datenschutz-Management - Organisatorische Maßnahmen** | |
|  |  |  |  |
| Software-Lösungen für Datenschutz-Management im Einsatz |  | Interner/externer Datenschutzbeauftragter  Name und Kontaktdaten: |  |
| Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (z.B. Wiki, Intranet usw.) |  | Mitarbeiter geschult und auf Datengeheimnis/Vertraulichkeit verpflichtet |  |
| Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12 oder alternatives Informationssicherheitskonzept |  | Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich) |  |
| Anderweitiges dokumentiertes Sicherheitskonzept |  | interner/externer Informationssicherheitsbeauftragter  Name und Kontaktdaten: |  |
| Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt |  | DSFA wird bei Bedarf durchgeführt |  |
|  |  | AVV kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach |  |
|  |  | formalisierter Prozess zur Bearbeitung von Auskunftsanfragen Betroffener |  |
|  |  | Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten |  |
|  |  | Gibt es ein Verzeichnis von Verarbeitungstätigkeiten i.S. de. Art. 30 Abs. 1 und 2 DSGVO |  |
|  |  |  |  |
| **b) Incident-Response-Management - Technische Maßnahmen** | | **Incident-Response-Management - Organisatorische Maßnahmen** | |
| Unterstützung bei der Reaktion auf Sicherheitsverletzungen | | | |
| Einsatz von Firewall und regelmässige Aktualisierung |  | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) |  |
| Einsatz von Spamfilter und regelmäßige Aktualisierung |  | Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen |  |
| Einsatz von Virenscanner und regelmäßige Aktualisierung |  | Einbindung von \_\_\_\_ DSB und \_\_\_\_ ISB in Sicherheitsvorfälle und Datenpannen |  |
| Intrusion Detection System (IDS) |  | Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem |  |
| Intrusion Prevention System (IPS) |  | Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen |  |
|  |  |  |  |
|  |  |  |  |
| **c) Datenschutzfreundliche Voreinstellungen - Technische Maßnahmen** | | **Datenschutzfreundliche Voreinstellungen - Organisatorische Maßnahmen** | |
| es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind |  |  |  |
| einfache Ausübung des Widerrufsrecht des Betroffenen durch technische Maßnahmen |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |