Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Die Verarbeitung ist geprüft und zertifiziert (bspw. BSI, ISO 27000) (Anhang oder Verweis)  Es liegt ein umfassendes Datensicherheitskonzept vor (Anhang oder Verweis)  Es liegt eine Beschreibung der für die Verarbeitung getroffenen Maßnahmen vor (Anhang oder Verweis)  Es wurden folgende Maßnahmen getroffen  (Erläutern Sie die zu den vorgegebenen Schutzzielen jeweils getroffenen Maßnahmen) | | | | | | | | | |
| **Psudonymisierung gemäß Art. 32 Abs. 1 lit. a) DSGVO** | | | | | | | | | |
| Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. | | | | | | | | | |
| Technische Maßnahmen | | | | | | Organisatorische Maßnahmen | | | |
|  | | Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. Verschlüsselt) | | | |  | Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren | | |
| Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | | | | |
| **Verschlüsselung gemäß Art. 32 Abs. 1 lit. b) DSGVO** | | | | | | | | | |
| Details und Maßnahmen bitte beschreiben: | | | | | | | | | |
| **Gewährleistung der Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO** | | | | | | | | | |
| **Zutrittskontrolle**  Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitsungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. | | | | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Manuelles Schließsystem | | |  | Schlüsselregelung / Liste |
|  | | |  | | Sicherheitsschlösser | | |  | Empfang / Rezeption / Pförtner |
|  | | |  | | Türen mit Knauf Außenseite | | |  | Besucherbuch / Protokoll der Besucher |
|  | | |  | | Automatisches Zugangskontrollsystem | | |  | Mitarbeiter- / Besucherausweise |
|  | | |  | | - Biometrische Zugangssperren | | |  | Besucher in Begleitung durch Mitarbeiter |
|  | | |  | | - Chipkarten / Transpondersysteme | | |  | Sorgfalt bei Auswahl des Wachpersonals |
|  | | |  | | - Schließsystem mit Codesperre | | |  | Sorgfalt bei Auswahl Reinigungsdienste |
|  | | |  | | Klingelanlage mit Kamera | | |  |  |
|  | | |  | | Videoüberwachung der Eingänge | | |  |  |
|  | | |  | | Alarmanlage | | |  |  |
|  | | |  | | Absicherung der Gebäudeschächte | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Zugangskontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.  Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Authentifizierungsverfahren | | |  | Verwalten von Benutzerberechtigungen |
|  | | |  | | - Login mit Benutzername + Passwort | | |  | Zentrales Zugangsmanagement und Passwortvergabe |
|  | | |  | | - Login mit biometrischen Daten | | |  | Lokale Benutzerverwaltung durch Administrator |
|  | | |  | | - Login mit Chipkarte / Zertifikat | | |  | Richtlinie „Sicheres Passwort“ |
|  | | |  | | - Tokenbasierte Authentifizierung | | |  | Anleitung „Manuelle Desktopsperre“ |
|  | | |  | | Automatische Desktopsperre | | |  | Erstellen von Benutzerprofilen |
|  | | |  | | Schutz der Rechner | | |  | Richtlinie „Löschen / Vernichten“ |
|  | | |  | | - Gehäuseverriegelung | | |  | Richtlinie „Clean desk“ |
|  | | |  | | - Sperre externer Schnittstellen (USB, Bluetooth, …) | | |  | Allg. Richtlinie Datenschutz und / oder Sicherheit |
|  | | |  | | - BIOS Schutz (separates Passwort) | | |  | Mobile Device Policy |
|  | | |  | | Anti-Viren-Software Server | | |  |  |
|  | | |  | | Anti-Virus-Software Clients | | |  |  |
|  | | |  | | Anti-Virus-Software mobile Geräte | | |  |  |
|  | | |  | | Firewall | | |  |  |
|  | | |  | | Einsatz VPN bei Remote-Zugriffen | | |  |  |
|  | | |  | | Schutz mobiler Geräte | | |  |  |
|  | | |  | | Mobile Device Management | | |  |  |
|  | | |  | | Intrusion Detection Systeme | | |  |  |
|  | | |  | | Verschlüsselung | | |  |  |
|  | | |  | | Verschlüsselung von Datenträgern | | |  |  |
|  | | |  | | Verschlüsselung Smartphones | | |  |  |
|  | | |  | | Verschlüsselung von Notebooks / Tablet | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Zugriffskontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Rollenbasierte Berechtigungsvergabe | | |  | Zentrales Berechtigungskonzept |
|  | | |  | | Vergabe und Änderung von Berechtigungen über ein zentrales Identitätsmanagement | | |  | Dezentrales Berechtigungskonzepte |
|  | | |  | | Aktenschredder (mind. Stufe 3, cross cut) | | |  | Verwaltung Benutzerrechte durch Administratoren |
|  | | |  | | Externer Aktenvernichter (DIN 32757) | | |  | Minimale Anzahl an Administratoren |
|  | | |  | | Physische Löschung von Datenträgern | | |  | Datenschutztresor |
|  | | |  | | Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Trennungskontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Trennung von Produktiv- und Testumgebung | | |  | Steuerung über Berechtigungskonzept |
|  | | |  | | Physikalische Trennung (Systeme / Datenbank / Datenträger) | | |  | Festlegung von Datenbankrechten |
|  | | |  | | Mandantenfähigkeit relevanter Anwendungen | | |  | Datensätze sind mit Zweckattributen versehen |
|  | | |  | | Sicherer Schnittstellenbetrieb | | |  | Schnittstellenbeschreibung |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Gewährleistung der Integrität gemäß Art. 32 Abs. 1 lit. b) DSGVO** | | | | | | | | | |
| **Weitergabekontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | E-Mail Verschlüsselung | | |  | Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen |
|  | | |  | | Bereitstellung über verschlüsselte Verbindungen wie sftp, https | | |  | Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen |
|  | | |  | | Nutzung von Signaturverfahren | | |  | Weitergabe in anonymisierter oder pseudonymisierter Form |
|  | | |  | | Einsatz von VPN | | |  | Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen |
|  | | |  | | Protokollierung der Zugriffe und Abrufe | | |  | Persönliche Übergabe mit Protokoll |
|  | | |  | | Sichere Transportbehälter | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Eingabekontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollieren erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | 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 ein Berechtigungskonzepts |
|  | | |  | |  | | |  | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden |
|  | | |  | |  | | |  | Klare Zuständigkeiten für Löschungen |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Gewährleistung der Verfügbarkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO** | | | | | | | | | |
|  | | | Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Feuer- und Rauchmeldeanlagen | | |  | Backup & Recovery-Konzept (ausformuliert) |
|  | | |  | | Feuerlöscher im Serverraum | | |  | Kontrolle des Sicherungsvorgangs |
|  | | |  | | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | | |  | Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |
|  | | |  | | Serverraum klimatisiert | | |  | Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums |
|  | | |  | | Unterbrechungsfreie Stromversorgung (USV) | | |  | Keine sanitären Anschlüsse im oder oberhalb des Serverraums |
|  | | |  | | Schutzsteckdosenleisten in Serverräumen | | |  | 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 |
|  | | |  | | Serverredundanz / Clustering | | |  |  |
|  | | |  | | RAID System / Festplattenspiegelung | | |  |  |
|  | | |  | | Videoüberwachung Serverraum | | |  |  |
|  | | |  | | Alarmmeldung bei unberechtigtem Zutritt zum Serverraum | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Gewährleistung der Belastbarkeit der Systeme gemäß Art. 32 Abs. 1 lit. b) DSGVO** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Einsatz vor Firewall und regelmäßige Aktualisierung | | |  | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber der Aufsichtsbehörde) |
|  | | |  | | Einsatz von Spamfilter und regelmäßige Aktualisierung | | |  | Dokumentierte Vorgehensweis 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 Datenpassen z.B. via Ticketsystem |
|  | | |  | | Intrusion Prevention System (IPS) | | |  | Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall gemäß Art. 32 Abs. 1 lit. c) DSGVO** | | | | | | | | | |
|  | | |  | | Umsetzung des BSI Standard 100-4 Notfallmanagement | | | | |
|  | | |  | | Notfallkonzept | | | | |
|  | | |  | | Notfallhandbuch | | | | |
|  | | |  | | Integration des Notfallmanagements in Geschäftsprozesse | | | | |
|  | | |  | | Durchführung von Notfallübungen | | | | |
|  | | |  | | Erprobung von Wiederanlaufszenarien | | | | |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 lit. d) DSGVO** | | | | | | | | | |
|  | | |  | | Regelmäßige Revision des Sicherheitskonzepts | | | | |
|  | | |  | | Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und –bewertung | | | | |
|  | | |  | | Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme | | | | |
|  | | |  | | Externe Prüfungen, Audits, Zertifizierungen | | | | |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Weitere Maßnahmen** | | | | | | | | | |
|  |  | | | Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. | | | | | |
|  |  | | | Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen. | | | | | |
|  |  | | | Sensibilisierung und/oder Schulung der an Verarbeitungsvorgängen Beteiligten | | | | | |
|  |  | | | Beteiligung des/der zuständigen Datenschutzbeauftragten | | | | | |
|  |  | | | Hinweis/Verpflichtung der an Verarbeitungsvorgängen Beteiligten auf das Datengeheimnis | | | | | |
|  |  | | | Folgende Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind: | | | | | |
|  |  | | | Im Falle einer Übermittlung oder Zweckänderung:  Folgende spezifischen Verfahrensregelungen werden getroffen, um die Einhaltung des LDSG und der DS-GVO sicherzustellen: | | | | | |
|  |  | | | Sonstiges: | | | | | |