Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

der Organisation

Stand

Auftraggeber

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. **Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO**
   1. Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.*

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Alarmanlage | Schlüsselregelung / Liste |
| Automatisches Zugangskontrollsystem | Empfang / Rezeption / Pförtner |
| Biometrische Zugangssperren | Besucherbuch / Protokoll der Besucher |
| Chipkarten / Transpondersysteme | Mitarbeiter- / Besucherausweise |
| Manuelles Schließsystem | Besucher in Begleitung durch Mitarbeiter |
| Sicherheitsschlösser | Sorgfalt bei Auswahl des Wachpersonals |
| Schließsystem mit Codesperre | Sorgfalt bei Auswahl Reinigungsdienste |
| Absicherung der Gebäudeschächte |  |
| Türen mit Knauf Außenseite |  |
| Klingelanlage mit Kamera |  |
| Videoüberwachung der Eingänge |  |
|  |  |
|  |  |
|  |  |

Weitere Maßnahmen bitte hier beschreiben:

* 1. 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. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).*

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Login mit Benutzername + Passwort | Verwalten von Benutzerberechtigungen |
| Login mit biometrischen Daten | Erstellen von Benutzerprofilen |
| Anti-Viren-Software Server | Zentrale Passwortvergabe |
| Anti-Virus-Software Clients | Richtlinie „Sicheres Passwort“ |
| Anti-Virus-Software mobile Geräte | Richtlinie „Löschen / Vernichten“ |
| Firewall | Richtlinie „Clean desk“ |
| Intrusion Detection Systeme | Allg. Richtlinie Datenschutz und / oder  Sicherheit |
| Mobile Device Management | Mobile Device Policy |
| Einsatz VPN bei Remote-Zugriffen | Anleitung „Manuelle Desktopsperre“ |
| Verschlüsselung von Datenträgern |  |
| Verschlüsselung Smartphones |  |
| Gehäuseverriegelung |  |
| BIOS Schutz (separates Passwort) |  |
| Sperre externer Schnittstellen (USB) |  |
| Automatische Desktopsperre |  |
| Verschlüsselung von Notebooks / Tablet |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. 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** |
| Aktenschredder (mind. Stufe 3, cross cut) | Einsatz Berechtigungskonzepte |
| 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 | Verwaltung Benutzerrechte durch  Administratoren |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. 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 Test-  umgebung | Steuerung über Berechtigungskonzept |
| Physikalische Trennung (Systeme /  Datenbanken / Datenträger) | Festlegung von Datenbankrechten |
| Mandantenfähigkeit relevanter  Anwendungen | Datensätze sind mit Zweckattributen ver-  sehen |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 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 Auf-  bewahrung in getrenntem und abge-  sicherten System (mögl. verschlüsselt) | Interne Anweisung, personenbezogene  Daten im Falle einer Weitergabe oder auch  nach Ablauf der gesetzlichen Löschfrist  möglichst zu anonymisieren / pseudonymi-  sieren |
|  |  |
|  |  |

Weitere Maßnahmen:

1. **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
   1. Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.*

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Email-Verschlüsselung (S/MIME / PGP)  Email-Signatur (S/MIME / PGP) | Dokumentation der Datenempfänger  sowie der Dauer der geplanten Über-  lassung bzw. der Löschfristen |
| Einsatz von VPN | Übersicht regelmäßiger Abruf- und  Übermittlungsvorgängen |
| Protokollierung der Zugriffe und Abrufe | Weitergabe in anonymisierter oder  pseudonymisierter Form |
| Sichere Transportbehälter | Sorgfalt bei Auswahl von Transport-  Personal und Fahrzeugen |
| Bereitstellung über verschlüsselte  Verbindungen wie sftp, https | Persönliche Übergabe mit Protokoll |
| Nutzung von Signaturverfahren |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. 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 Protokollierungen 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 eines Berechtigungskonzepts |
|  | Aufbewahrung von Formularen, von  denen Daten in automatisierte Verar-  beitungen übernommen wurden |
|  | Klare Zuständigkeiten für Löschungen |

Weitere Maßnahmen:

1. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**
   1. Verfügbarkeitskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.*

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Feuer- und Rauchmeldeanlagen | Backup & Recovery-Konzept (ausformuliert) |
| Feuerlöscher Serverraum | Kontrolle des Sicherungsvorgangs |
| Serverraumüberwachung Temperatur  und Feuchtigkeit | Regelmäßige Tests zur Datenwiederher-  Herstellung 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 Quell-  dichtung etc.) | Getrennte Partitionen für Betriebs-  systeme und Daten |
| RAID System / Festplattenspiegelung |  |
| Videoüberwachung Serverraum |  |
| Alarmmeldung bei unberechtigtem Zutritt  zu Serverraum |  |
|  |  |
|  |  |
|  |  |

Weitere Maßnahmen:

1. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**
   1. Datenschutz-Management

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Software-Lösungen für Datenschutz-  Management im Einsatz | Interner / externer Datenschutzbeauftragter  Name / Firma / Kontaktdaten |
| Zentrale Dokumentation aller Verfahrens-  weisen und Regelungen zum Datenschutz  mit Zugriffsmöglichkeit für Mitarbeiter nach  Bedarf / Berechtigung (z.B. Wiki, Intranet …) | Mitarbeiter geschult und auf  Vertraulichkeit / Datengeheimnis  verpflichtet |
| Sicherheitszertifizierung nach ISO 27001,  BSI IT-Grundschutz oder ISIS12  Alternatives Informationssicherheits-  konzept | Regelmäßige Sensibilisierung der  Mitarbeiter  Mindestens jährlich |
| Anderweitiges dokumentiertes Sicherheits-  Konzept | Interner / externer Informationssicherheits-  Beauftragter Name / Firma Kontakt |
| Eine Überprüfung der Wirksamkeit der  Technischen Schutzmaßnahmen wird mind.  jährlich durchgeführt | Die Datenschutz-Folgenabschätzung (DSFA)  wird bei Bedarf durchgeführt |
|  | Die Organisation kommt den Informations-  pflichten nach Art. 13 und 14 DSGVO nach |
|  | Formalisierter Prozeß zur Bearbeitung von  Auskunftsanfragen seitens Betroffener ist  vorhanden |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen*

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| 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 Sicherheitsvor-  fällen und Datenpannen |
|  |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

*Privacy by design / Privacy by default*

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Es werden nicht mehr personenbezogene  Daten erhoben, als für den jeweiligen Zweck  erforderlich sind |  |
| Einfache Ausübung des Widerrufrechts  des Betroffenen durch technische Maß-  nahmen |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Auftragskontrolle (Outsourcing an Dritte)

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.* *Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.*

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  | Vorherige Prüfung der vom Auftrag-  nehmer getroffenen Sicherheitsmaß-  nahmen und deren Dokumentation |
|  | Auswahl des Auftragnehmers unter  Sorgfaltsgesichtspunkten (gerade in  Bezug auf Datenschutz und Datensicher-  heit |
|  | Abschluss der notwendigen Vereinbarung  zur Auftragsverarbeitung bzw. EU Standard-  Vertragsklauseln |
|  | Schriftliche Weisungen an den Auftrag-  nehmer |
|  | Verpflichtung der Mitarbeiter des Auftrag-  nehmers auf Datengeheimnis |
|  | Verpflichtung zur Bestellung eines Daten-  schutzbeauftragten durch den Auftrag-  nehmer bei Vorliegen Bestellpflicht |
|  | Vereinbarung wirksamer Kontrollrechte  gegenüber dem Auftragnehmer |
|  | Regelung zum Einsatz weiterer Sub-  unternehmer |
|  | Sicherstellung der Vernichtung von Daten  nach Beendigung des Auftrags |
|  | Bei längerer Zusammenarbeit: Laufende  Überprüfung des Auftragnehmers und  seines Schutzniveaus |

Weitere Maßnahmen:

alternativ:

Hiermit versichern wir, keine Subunternehmer im Sinne einer

Auftragsverarbeitung einzusetzen.

1. Anlagen (optional)

Verzeichnis zu den Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten

(Art. 30 Abs. 2 DSGVO)

Liste der eingesetzten Subunternehmer mit Tätigkeiten für Sie als Auftraggeber

Richtlinie Datenschutz

Richtlinie Umgang mit Datenpannen

Übersicht der Sensibilisierungs- und Schulungsmaßnahmen der letzten 24 Monate

Bitte fügen Sie nichts bei, was bei unberechtigter Kenntnisnahme ein Sicherheitsrisiko für Ihre Organisation darstellen kann.

**Ausgefüllt für die Organisation durch**

Name

Funktion

Rufnummer

Email

Ort, Datum

**Vom Auftraggeber auszufüllen:**

Geprüft am       durch      . Ergebnis(se):

Es besteht noch Klärungsbedarf zu

TOM sind für den angestrebten Schutzzweck ausreichend

Vereinbarung Auftragsverarbeitung kann geschlossen werden

*Kurzfassung der Nutzungsregeln: Diese Checkliste kann gerne in der Praxis von Unternehmen oder auch Behörden / kommunalen Einrichtungen genutzt und verändert werden. Ich möchte jedoch nicht, dass diese Checkliste ohne unsere Zustimmung auf anderen Internetseiten als Muster zum Download angeboten wird oder sich irgendwann in einem käuflich zu erwerbenden Vorlagenbuch wiederfindet. Es wird keine Haftung für Schäden durch die Verwendung der Checkliste übernommen.*