Technische und organisatorische Maßnahmen

1. Vertraulichkeit

➢ Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

Zutritt zu den Büroräumlichkeiten

- Das Bürogebäude ist zwischen 19.00 Uhr und 07.00 Uhr verschlossen (sonntags ganztätig).
- Dokumentierte Schlüsselvergabe und -entzug an Mitarbeiter.
- Der Hausgang wird durch eine Videokamera überwacht (von GF).
- Türsicherung – verschlossene Bürotüren, auch bei kurzer Abwesenheit.
- Zur Auftragserfüllung verwendete Geräte und Unterlagen werden jederzeit sicher vor Unbefugten aufbewahrt.

➢ Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und Verfahren gehindert werden. Diese beziehen sich – im Gegensatz zur Zutrittskontrolle – auf das Eindringen unbefugter Personen in das EDV-System selbst:

Zugang Interne Systeme

- Professioneller Firewallschutz besteht an den Unternehmenszugängen
- Passwortgesicherter Bildschirmschoner sind im Einsatz. Bei Verlassen des Büros wird der Bildschirm gesperrt.
- Die Identifikation am Terminalserver erfolgt personenbezogen.
- Die Benutzeridentifikation erfolgt mittels individuellem Benutzernamen und Passwort.
- Zugang ist passwortgeschützt
- Zugang besteht nur für Mitarbeiter
- Verwendete Passwörter müssen eine Mindestmenge haben.
- Passwörter werden in regelmäßigen Abständen erneuert.
- Wechseldatenträger, die das Unternehmen verlassen, werden verschlüsselt.

- Personenbezogene Daten von Auftraggebern werden nur auf Datenträgern des Auftragnehmers gespeichert. Zum Vertragsende dürfen auf Anweisung des Auftraggebers ein mobiler Datenträger mit den personenbezogenen Daten erstellt und versandt werden.
- Es wird in angemessenen Umfang über die datenschutzkonforme Nutzung von Datenträgern und Notebooks informiert und aktuell gehalten.

Zugang auf Cloud-Lösungen

- Passwörter sind nur dem Auftraggeber bekannt.
- Sperrung von Terminals
- Zuordnung einzelner Terminals und/oder Terminalnutzer ausschließlich für spezielle Funktionen
- Regelungen für Benutzerberechtigung
- Verpflichtungen der Mitarbeiter auf das Datengeheimnis
- Nutzercodes für Daten und Programme
- Differenzierte Zugangsregelungen (z.B. durch Zugriffsegmentsperren)
- Führen eines Logbuchs
- Kontrollierte Vernichtung von Datenträgern
- Arbeitsabweisungen für Datenerfassungsvorlagen
- Prüf-, Abstimm- und Kontrollsysteme
- Der elektronische Datenaustausch erfolgt unter Einsatz von Sicherungssystemen mit mehrfachen und komplexen Prüfungsabläufen. Anhand von Firewalls, Proxy Servern, VPN Routern und Analysesystemen erfolgt die technische Absicherung der Verbindungen. Hierzu werden für das Rechenzentrum wirtschaftlich, vertretbare, geeignete Verschlüsselungstechnologien eingesetzt.

➢ 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:

Bei internen Verwaltungssystemen

- Die Rechte auf dem Terminalserver werden durch den Verantwortlichen bestimmt
- Durch regelmäßige Sicherheitsupdates und verschlüsselte Backups, wird sichergestellt, dass unberechtigte Zugriffe verhindert werden.
- Zugang zum Terminalserver erfolgt nur mit individuellem Benutzernamen und Passwort.
- Die Passwortvorgaben sind technisch erzwungen. Es werden mindestens folgende Vorgaben umgesetzt:
    - Bestehend aus 8 Zeichen
    - Kombination aus Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern (mind. 3 von 4 Kriterien)
    - Ausschluss von Trivialpasswörtern
    - Sperrung des Accounts nach 3 fehlgeschlagenen Anmeldeversuchen
- Bei Zuteilung von Passwörtern ändert der Benutzer zu Beginn der Nutzung das Passwort.
- Diese Vorgaben werden durch den Verantwortlichen technisch umgesetzt.
- Passwörter werden geheim gehalten und sind nur dem Benutzer persönlich bekannt. Insbesondere werden Passwörter nicht notiert oder ungeschützt gespeichert.
- Im Rahmen der Auftragserfüllung verwendete Passwörter unterscheiden sich von anderen aktuellen oder ehemaligen Passwörtern und werden ausnahmslos nur für die Auftragserledigung verwendet.
- Nach 10 Minuten Inaktivität erfolgt ein Verbindungs-Time-Out
- Protokollierung bei Zugriff auf eine Anwendung bzw. eine Datenbank.
- Die Protokollierung bei Zugriff auf eine Anwendung bzw. eine Datenbank erfolgt durch den Verantwortlichen.

Bei Cloud-Lösungen

- Der Verantwortliche stellt sicher, dass die von ihm vergebenen Passwörter nur berechtigten Personen zur Verfügung gestellt werden.
- Autorisierungskonzepte
- Identifikation des Terminals/des Terminalnutzers im System
- Automatische Abschaltung der User ID bei mehrmaliger fehlerhafter Eingabe des Passworts.
- Logfiles (Überwachung von Einbruchsversuchens)
- Festlegung des zugriffsberechtigten Personals
- Schützende Maßnahmen für die Datenspeicherung, sowie für das Lesen, Sperrung und die Löschung gespeicherter Daten.
- Verschlüsselung von Sicherheitsdaten
- Trennung von Produktions- und Testumgebung für Bibliotheken und Dateien.
- Sorge dafür tragen, dass die Eintragungen zur Datenverarbeitung (Räume, Gebäude, Computerhardware und dazugehöriges Equipment) abgeschlossen werden können
- Bestimmung der Person in solchen Bereichen, die für die Entfernung von Datenträgern autorisiert sind.
- Kontrolle der Entfernung von Datenträgern
- Sicherung der Bereiche, in denen Datenträger untergebracht sind
- Herausgabe von Datenträgern ausschließlich an autorisierte Personen
- Kontrolle der Daten, kontrollierte und dokumentierte Vernichtung von Datenträgern

➢ Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Trennung von Entwicklungs-, Tests- und Produktivsystem bei internen Verwaltungssystemen

- Eine angemessene Trennung der Systeme bzw. Datenbanken erfolgt durch den Verantwortlichen
- Berechtigte Mitarbeiter sollen auf alle Kunden zugreifen können
- Personal- und Verwaltungsdaten werden separat aufbewahrt

Bei Cloud Lösungen

- Speicherung der Daten in getrennten Archiven
- Logische Trennung der verschiedenen Datentöpfe
- Sicherstellung, dass keine Überschneidung von Datenbeständen einzelner Kunden möglich ist und dass Daten eines Kunden von anderen Kunden nicht ausgelesen werden können.

➢ Pseudonymisierung (Art. 32 Abs.1 lit. a und Art. 25 Abs. 1 DS-GVO)

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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

- Einsatz einer geeigneten Festplattenverschlüsselung für Notebooks mit denen der Zugang zum *remote* ermöglicht wird.
- Sämtliche personenbezogenen Daten

2. Integrität

➢ Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Bei internen Verwaltungssystemen

- Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Verschlüsselte Datenübertragung der Email-Anhänge (passwortgestützt)
- Verschlüsselte Email-Kommunikation mit allen Kunden
- Ein Fernzugriff auf Daten findet nur IP Sec VPN oder durch den Einsatz eines gleich oder höherwertigen Systems statt

Bei Cloud Lösungen

- Bestimmung befugter Personen
- Interne Anforderungen zur Verifizierung (Vieraugenprinzip)
- Kontrolle der Dateien
- Sicherheitsschränke
- Kontrollierte Vernichtung der Datenträger
- Dokumentation der Übermittlungsprogramme
- Autorisierungsrichtlinien
- Vollständigkeits- und Richtigkeitsprüfung des Datentransfers
- Verschlüsselung

➢ Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Bei internen Verwaltungssystemen

- Die Daten werden vom Verantwortlichen selbst eingegeben bzw. erfasst
- Dokumentationen von Veränderungen in Anwendungen und anderen Daten bestehen
- Änderungen werden protokolliert und können nachvollzogen werden
- Auf lokalen Rechnern werden keine personenbezogenen Daten gespeichert

Bei Cloud-Lösungen

- Die Daten werden vom Verantwortlichen selbst eingegeben bzw. erfasst
- Quittierung des Dateneingangs
- Elektronische Protokollierung der Datenverarbeitung, insbesondere die Nutzung der Daten

3. Verfügbarkeit und Belastbarkeit

➢ Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

Bei internen Verwaltungssystemen

- Backup- und Recoverykonzept mit täglicher Sicherung der relevanten Daten

- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme und SPAM-Filter)
- Einsatz Festplattenspiegelung
- Daten werden physikalisch und logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen
- Überbrückung der Stromversorgung bei Ausfall mittels USV
- Räumlich getrennt Aufbewahrung von Sicherungsdatenträgern

Bei Cloud-Lösungen

- Backup-Verfahren (RAID-Verfahren, Bandsicherung im feuerfesten Tresor etc.)
- Unterbrechungsfreie Stromversorgung mittels USV
- Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme und SPAM-Filter)
- Brand- und Wasserschutzeinrichtung (Feuerlöschanlagen, Brandschutztüren, Rauchmelder etc.)
- Einbruchmeldeanlagen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

➢ Datenschutzmanagement

Maßnahmen, die gewährleisten, dass die Datenschutzanforderungen umgesetzt werden und auch nachweisbar sind:

- Ein Datenschutzbeauftragter ist bestellt
- Der Datenschutzbeauftragte schult regelmäßig die Mitarbeiter
- Verarbeitungsübersichten werden regelmäßig gepflegt
- Der Verantwortliche ist für die vollständige Umsetzung der Grundsätze der IT-Sicherheit und für die Erfüllung der an ihn gestellten IT-Sicherheitsaufgaben verantwortlich.
- Ein Datenschutzkonzept dient als Grundlage für die Datenschutzorganisation

➢ Incident-Response-Management

Maßnahmen, die gewährleisten, dass Datenpannen schnell erkannt und gemeldet werden:

- Der Verantwortliche verfügt über einen geregelten bestehenden Prozess für die Handhabung von Informationssicherheits- und Datenschutzvorfällen, um

diesbezüglich eine konsistente und wirksame Herangehensweise zu gewährleisten

- Auftragskontrolle

Bei internen Verwaltungssystemen

- Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag.
- Die Vertragsdurchführung erfolgt weisungsgebunden

Bei Cloud-Lösungen

- Es findet eine eindeutige Vertragsgestaltung statt
- Es wird eine geeignete Auswahl von Partnerunternehmen hinsichtlich der getroffenen technisch-organisatorischen Maßnahmen getroffen
- Umsetzung klarer Regelungen von Verantwortlichkeiten
- Die Auftragserteilung erfolgt nach spezifischen Regeln
- Die Vertragsdurchführung erfolgt weisungsgebunden und wird regelmäßig kontrolliert.

- Organisationskontrolle

Bei Cloud-Lösungen

- Interne Datenverarbeitungsrichtlinien und -verfahren, Arbeitsanweisungen, Prozessbeschreibungen und Regelungen für Tests und Freigabe neuer Verfahren, sofern übermittelte Daten betroffen sind.
- Nutzung von branchenüblichen Standardsystemen und Programmprüfung, sowie geeigneter Individualsoftware
- Formulierung eines Notfallplans

- Weisungskontrolle

Bei Cloud-Lösungen

- Für die Mitarbeiter bindende Richtlinien und Arbeitsanweisungen, die sich aus dem jeweiligen verfahren ergeben
- Auskunftserteilung zu speziellen Verfahren oder Daten auf Anfrage