Technische und Organisatorische Maßnahmen

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

1.1 // Zutrittskontrolle

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist verboten. Das ist der Grundsatz der Datenschutzgrundverordnung. Eine Ausnahme besteht nur dann, wenn es eine ausdrückliche gesetzliche Regelung dafür gibt oder der Betroffene freiwillig in die Verarbeitung seiner Daten eingewilligt hat. Unter Zutrittskontrolle verstehen wir Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Technisch-Organisatorische Maßnahmen:

- Automatisches Zutrittskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Schließsystem mit Codesperre
- Personenkontrolle am Empfang
- Sorgfältige Auswahl Reinigungspersonal
- Schließsystem mit Codesperre
- Sorgfältige Auswahl Wachpersonal
- Schriftliche Schlüsselregelung

1.2 // Zugangskontrolle

Unter Zugangskontrolle verstehen wir Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
Technisch-Organisatorische Maßnahmen:

- Authentifizierung von Benutzername und Passwort
- Zuordnung von Benutzerrechten
- Festplattenverschlüsselung
- Verschlüsselte Smartphone Inhalte
- Zentrale Verwaltung der Mobile Devices
- Einsatz von Firewalls
- Erstellung von Benutzerprofilen
- Zuordnung Benutzerprofile zu IT-Systemen
- Keine unpersonalisierten Accounts
- Einsatz von Anti-Virensoftware

1.3 // Zugriffskontrolle

Unter Zugriffskontrolle verstehen wir Maßnahmen, die gewährleisten, dass die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert und verändert oder entfernt werden können
Technisch-Organisatorische Maßnahmen:

- Umgesetztes Rollenkonzept im AD
- Protokollierung aller wichtigen Events
- Einsatz von Aktenvernichtern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Reduzierte Anzahl von Administratoren
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Auslagerung von Sicherungsdatenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

- Protokollierung der Vernichtung

1.4 // Trennungskontrolle

Unter Trennungskontrolle verstehen wir Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:
Technisch-Organisatorische Maßnahmen:

- physikalisch getrennte Speicherung auf gesonderten Systemen
- Trennung von Produktiv und Testsystem
- Logische Mandantentrennung
- Festlegung von Datenbankrechten

1.5 // Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Unter Pseudonymisierung verstehen wir Maßnahmen, die gewährleisten, dass die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.
Technisch-Organisatorische Maßnahmen:

- Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

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

2.1 // Weitergabekontrolle

Unter Weitergabekontrolle verstehen wir 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Technisch-Organisatorische Maßnahmen:

- E-Mail Verschlüsselung
- Nutzung von Standleitungen und VPN Tunneln
- Bei physischen Transporten Auswahl von Transportpersonal und –fahrzeugen sowie sicheren Tranportbehältern
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

2.2 // Eingabekontrolle

Unter Eingabekontrolle verstehen wir Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
Technisch-Organisatorische Maßnahmen:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Rechtevergabe hierzu auf Basis des abgestimmten Berechtigungskonzeptes
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Einrichtung ausschließlich personalisierter Useraccounts

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

3.1 // Verfügbarkeitskontrolle

Unter Verfügbarkeitskontrolle verstehen wir Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Da wir Systeme mit personenbezogenen Daten und Systeme ohne personenbezogene Daten nicht unterschiedlich handhaben wollen, haben wir beschlossen alle Systeme so zu behandeln, als würden sie personenbezogene Daten verarbeiten. Dies stellt für uns eine Erhöhung der Gesamtsicherheit und eine Verbesserung der Verwaltungsprozesse dar.
Technisch-Organisatorische Maßnahmen:

- Redundante virtuelle Systeme
- Nutzung von zwei getrennten Rechenzentren
- Nutzung eines Notfallrechenzentrums
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräume
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- USV gesicherte Rechenzentren

3.2 // Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Technisch-organisatorische Maßnahmen:

- IT-Notfallplan
- Durchführung von Notfalltests

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

Unter Überprüfungs-, Bewertungs- und Evaluierungsverfahren verstehen wir Maßnahmen, die gewährleisten, dass die sichere Verarbeitung personenbezogener Daten wirksam durchgeführt wird. Dazu zählen auch solche Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
Technisch-organisatorische Maßnahmen:

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle
- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten
- Vorherige Überprüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Fortlaufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags