Technische und organisatorische Maßnahmen der Mahr EDV GmbH zum Datenschutz
Anlage zur Vereinbarung zur Auftragsdatenverarbeitung

Mahr EDV hat umfassende Sicherheitsvorkehrungen und Maßnahmen getroffen, um vertrauliche und/oder personenbezogene Daten effektiv zu schützen. Seit Gründung der Mahr EDV im Jahre 1999 kam es zu keinem einzigen Datenschutzvorfall. Im Folgenden sind wesentliche Maßnahmen beschrieben.

Bereich / Ziel	**Maßnahmen** (max. 10)	
Auftragskontrolle		
Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	✓ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten	✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
	✓ Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen	✓ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
	✓ Schriftliche Weisungen an den Auftragnehmer	✓ Vertragsstrafen bei Verstößen
	✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis	✓ Auftragsverarbeitungsvereinbarung
	✓ Auftragnehmer hat Datenschutzbeauftragten bestellt	✓ Schulung, Prüfung, Besichtigung
Datenschutz-Management		
Gewährleistung des Daten- und Vertraulichkeitsschutzes durch regelmäßige Prüfung und Evaluierung	✓ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung	✓ Mitarbeiterschulungen
	✓ Sicherheitskonzept	✓ Verpflichtungsvereinbarungen zum Datenschutz
	✓ Bestellung eines Datenschutzbeauftragten	✓ Regelmäßige Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen
	✓ Datenschutz-Folgenabschätzung	✓ Revisionierung
	✓ Erfüllung der Informationspflichten gemäß BDSG/DSVGO	✓ Löschssperren

Eingabekontrolle		
Protokollierung auch zur nachträglichen Prüfung, ob, wer und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt hat.	✓ Protokollierung der Eingabe, Änderung und Löschung von Daten ✓ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind ✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts ✓ Monitoring	✓ Klare Verantwortung für Löschungen ✓ Klare Verantwortung für Löschungen Sperrungen ✓ Passwortschutz ✓ Benutzerauthentifizierung ✓ Regelmäßige Sicherheitsprüfungen
Incident-Response-Management		
Gewährleistung einer strukturierten Reaktion auf Sicherheitsverletzungen	✓ Firewall ✓ Virenschutz ✓ Spamfilter ✓ Intrusion Prevention System ✓ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen	✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen ✓ Einbindung von DSB ✓ Dokumentation von Sicherheitsvorfällen ✓ Ticketsystem ✓ Regelmäßige Sicherheitsprüfungen
Privacy by Design		
Voreinstellung von Systemen zur Datensparsamkeit	✓ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind ✓ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

Pseudonymisierung		
Sicherstellung, dass Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können	✓ 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	
Trennungskontrolle		
Sicherstellung, dass zu unterschiedlichen Zwecken erhobene Daten nur getrennt verarbeitet werden können.	✓ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern ✓ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden ✓ Erstellung eines Berechtigungskonzepts ✓ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System ✓ Versehen der Datensätze mit Zweckattributen/Datenfeldern	✓ Trennung von Produktiv- und Testsystem ✓ Festlegung von Datenbankrechten ✓ Logische Mandantentrennung (softwareseitig) ✓ Festlegung von Datenbankrechten
Verfügbarkeitskontrolle		
Schutz der Daten vor zufälliger Zerstörung oder Verlust.	✓ USV und Notstrom ✓ Klimaanlage und Temperatur- und Feuchtemonitoring in Serverräumen ✓ RAID Systeme und Komponentenredundanz, RZ-Redundanz ✓ Schutzsteckdosen ✓ Brandfrüherkennung, Feuerlöschung	✓ Bewegungsmelder, Videoüberwachung, 24/7 Aufschaltung zum Sicherheitsdienst ✓ Backup- & Recoverykonzept, Havariepläne ✓ Regelmäßiger Test und Protokollierung Datenwiederherstellung ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Weitergabekontrolle		
Schutz der Daten auf jeglichen Transportwegen vor dem Zugriff Dritter (einschließlich des Lesens, Kopierens, Änderns, Entfernens) und Sicherstellung der Nachvollziehbarkeit sämtlicher Datenweitergaben.	✓ Einrichtung von verschlüsselten VPN-Tunneln ✓ Elektronische Verschlüsselung ✓ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form ✓ Verwendung sicherer Transportbehälter/-verpackungen ✓ Protokollierung der Nutzung	✓ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen ✓ Verfahrensverzeichnis
Zugangskontrolle		
Beschränkung der Nutzung von Datenverarbeitungsanlagen auf Befugte	✓ Benutzerrollen und Rechte geregelt, zugeordnet zu Systemen/Anwendungen, Authentifikation mit Benutzername/Passwort ✓ Passwortkomplexitätsrichtlinien, Passwortänderungsrichtlinien und -überwachung bzw. automatische Zugangssperre ✓ Sicherheitsschlösser/Verriegelungen (physisch), Abschaltung von Schnittstellen (bspw. USB) ✓ VPN/Verschlüsselung/https ✓ Schlüsselregelung	✓ Verschlüsselung von PCs ,Notebooks, Datenträgern, Smartphones ✓ Sorgfältige Auswahl von Wach- und Reinigungspersonal (ggf. begleiteter Zugang) ✓ Mobile Device Management ✓ Intrustion-Detection-Systeme, Firewalls, Virenschutz ✓ Benutzerschulungen
Zugriffskontrolle		
Beschränkung des Zugriffs auch berechtigter Nutzer von Datenverarbeitungsanlagen auf die jeweils notwendigen Daten.	✓ Berechtigungsstufen und -konzepte ✓ Verschlüsselung von Datenträgern ✓ Anzahl der Administratoren auf das Notwendigste reduziert ✓ Verwaltung der Rechte durch Systemadministrator ✓ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	✓ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel ✓ Physische Löschung von Datenträgern vor Wiederverwendung ✓ Sichere Aufbewahrung von Datenträgern ✓ Einsatz von Aktenvernichtern bzw. Dienstleistern ✓ Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

Zutrittskontrolle		
Beschränkung des Zutritts zu Datenverarbeitungsanlagen auf Befugte	✓ Alarmanlage	✓ Sorgfältige Auswahl von Wachpersonal/Reinigungsdiensten
	✓ Automatisches Zugangskontrollsystem	✓ Absicherung von Gebäudeschächten
	✓ Schließsystem mit Codesperre	✓ Videoüberwachung
	✓ Lichtschranken / Bewegungsmelder	✓ Sicherheitsschlösser
	✓ Schlüsselregelung (Schlüsselausgabe etc.)	✓ Empfang und Besucherbegleitung