Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

1. Zutrittskontrolle

Die Zutrittskontrolle stellt sicher, dass Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen (Gebäude, Büros, …) haben.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Alarmanlage		Anmeldung / Personenkontrolle beim Pförtner / Empfang
	Lichtschranken / Bewegungsmelder		Protokollierung der Besucher / Besucherbuch
	Außenzugänge videoüberwacht		Tragepflicht von Gästeausweisen
	Außenzugänge immer verschlossen		Regelung, dass sich Besucher nicht unbeaufsichtigt bewegen können
	Schließsystem mit biometrischer Authentifizierung		Dokumentation ausgegebener Transponder / Schlüssel
	Schließsystem mit Authentifizierung per Chipkarten / Transponder		Zutrittskonzept für unterschiedliche Bereiche (z.B. verschlossene Büros / Räume / Schränke) C
	Schließsystem mit Authentifizierung per Passwort		Tragepflicht von Mitarbeiterausweisen
	Sicherheitsschlösser		Sorgfältige Auswahl von Reinigungspersonal
	Absicherung von Gebäudeschächten / Lüftungskanälen		Sorgfältige Auswahl von Sicherheitspersonal
	Weitere: _____		Weitere: _____

besondere Relevanz bei mobilem Arbeiten

2. Zugangskontrolle

Die Zugangskontrolle stellt sicher, dass Unbefugte keinen Zugang zu Datenverarbeitungsanlagen (PCs, Smartphones…) haben.

	Technische Maßnahmen		Organisatorische Maßnahmen	
D	Authentifizierung mit Kennung und Passwort		Anzahl der Administratoren minimiert	
D	Authentifizierung mit biometrischen Verfahren		Keine lokalen Adminrechte für Benutzer	
	Authentifizierung nach Bildschirmschoner		Dokumentiertes Benutzerkonzept (Freigabe, Anlage, Änderung, Löschung)	
G	Zwei-Faktor-Authentifizierung (z.B. Einmalpasswort per SMS)		Richtlinie bzgl. Passwörter (Komplexität, versch. Passwörter je Anwendung, Weitergabeverbot)	D
	Einsatz von Anti-Viren-Software		Richtlinie bzgl. Sperrung von Rechnern / Laptops	D
	Einsatz einer Hardware-Firewall		Richtlinie bzgl. Sperrung von Smartphones / Tablets	D
	Einsatz einer Software-Firewall		Richtlinie bzgl. sicheren Speicherorten von Daten	E
	Einsatz einer zentralen Smartphone-Admin-Software (Mobile Device Management)		Richtlinie bzgl. der sicheren Aufbewahrung von externen Datenträgern	
E	Einsatz von VPN-Verbindungen bei Zugriff von Extern		Datenschutzkonforme Videokonferenzen (z.B: Einwilligung bei Aufzeichnung)	A
	Sperren von externen Schnittstellen (z.B. USB)		Vertraulichkeit bei Bildschirmfreigaben und Videokonferenzen	B
	Verschlüsselung von Datenträgern in PCs		Laptops / Monitore sichtgeschützt aufstellen	
	Verschlüsselung von Datenträgern in Laptops		Vertraulichkeit bei Telefonaten / Videokonferenzen in der Öffentlichkeit	B
	Verschlüsselung von Smartphones / Tablets		Clean-Desk-Policy (Aufgeräumter Arbeitsplatz beim Verlassen)	C
	Verschlüsselung von anderen mobilen Datenträgern		Weitere: _____	
	Geplante Installation von Softwarepatches			
F	Geplante Installation von Softwarepatches auch außerhalb des Firmennetzwerkes			
	Weitere: _____			

Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

3. Zugriffskontrolle

Die Zugriffskontrolle stellt sicher, dass nur berechtigte Personen auf benötigte Daten zugreifen können.

	Technische Maßnahmen		Organisatorische Maßnahmen
C	Einsatz von Papier-Aktenvernichtern (gem. DIN 66399)		Einsatz von Dienstleistern zur Datenträger-Vernichtung nach DIN 66399 (inkl. Protokoll)
	Mechanische Zerstörung von Datenträgern		Einsatz von Dienstleistern zur Papierakten-Vernichtung nach DIN 66399 (inkl. Protokoll)
	Physische Löschung von Datenträgern vor Wiederverwendung		Regelung der Nutzerzugriffe (Zuordnung Nutzer - IT-Systeme)
	Ausdruck nur bei Authentifizierung am Drucker		Regelmäßiges Review des Berechtigungskonzepts
	Weitere: _____		Weitere: _____

4. Weitergabekontrolle

Die Weitergabekontrolle stellt sicher, dass Datenströme und Änderungen an Daten jederzeit nachvollzogen werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen	
E	Einsatz von VPN-Verbindungen bei Zugriff von Extern		Dokumentation der Empfänger von Daten inkl. Zeitspannen der Überlassung bzw. Löschung	
E	Verschlüsselung von E-Mails		Weitergabe von Daten in anonymisierter oder pseudonymisierter Form	E
E	Verschlüsselung von Email-Anhängen		Dokumentation und Prüfung automatischer Abruf- und Übermittlungsvorgänge	
E	Sichere Übertragung über Software (z.B. zur Bank / Steuerberater)		Prüfung Logfiles (Fileserver, Mail, Sonstige Transfers)	
E	Sichere Übertragung über Clouds / Managed File Transfer		Sorgfältige Auswahl von Transportpersonal und -fahrzeugen	
	Datenexport-Funktion bei kritischen Systemen eingeschränkt / deaktiviert		Sichere Transportbehälter/-verpackungen	
	Weitere: _____		Weitere: _____	

5. Eingabekontrolle

Die Eingabekontrolle stellt sicher, dass nachvollzogen werden kann, wer Daten eingegeben, geändert oder gelöscht hat.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Protokollierung von Eingabe, Änderung und Löschung von Daten durch Benutzernamen		Aufbewahrung von Formularen, von denen Daten in IT-Systeme übernommen wurden
	Weitere: _____		Weitere: _____

6. Auftragskontrolle

Die Auftragskontrolle stellt sicher, dass Auftragnehmer die Daten ausschließlich nach Vorgaben des Verantwortlichen verarbeiten.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Weitere: _____		Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
			DSGVO-konforme Weisung an den Auftrag-nehmer (Vereinbarung Auftragsverarbeitung)
			Sicherstellung der Rückgabe / Vernichtung von Daten nach Beendigung des Auftrags
			Vertragsstrafen bei Verstößen
			Prüfung der Sicherheitsmaßnahmen des Auftragnehmer vor / während Auftrag
			Weitere: _____

7. Verfügbarkeits- und Belastbarkeitskontrolle

Die Verfügbarkeitskontrolle stellt sicher, dass Daten gegen zufällige Zerstörung geschützt sind.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Klimaanlage in Serverräumen		Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
	Anlagen zur Überwachung von Feuer- und Rauch in Serverräumen		Sichere Anordnung der Serverräume (Wasserleitungen, Hochwasser)
	Anlagen zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen		Sichere Anordnung der Serverräume (in verschiedenen Gebäuden / Brandabschnitten)
	CO_2-Feuerlöschgeräte in / neben Serverräumen		Durchführung von Belastungstests (z.B. Stromausfall / USV, Ausfall redundanter Server)
	Separater Stromkreis für Server		Durchführung von Belastungstests (z.B. Penetration)
	Schutzsteckdosenleisten in Serverräumen		Erstellen und Umsetzen eines Notfallplans
	Unterbrechungsfreie Stromversorgung (USV), welche die Server kontrolliert abschaltet		Erstellen und Umsetzen eines Backup- & Recoverykonzepts
	Unterbrechungsfreie Stromversorgung (USV) ohne automatische Abschaltung der Server		Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
	Redundante Server		Aufbewahrung von Datensicherung an einem sicheren Ort im Unternehmen
	Redundante Serverdatenträger (z.B. RAID 1)		Durchführung von regelmäßigen Datenwiederherstellungstests
	Verschlüsselung von Datensicherungen		Server-Monitoring mit Meldung an Admin bei Störungen (SMS, Email)
	Weitere: _____		Weitere: _____

E

besondere Relevanz bei mobilem Arbeiten

8. Trennungsgebot

Die Trennungskontrolle stellt sicher, dass unterschiedlich erhobene Daten auch getrennt verarbeitet werden.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Pseudonymisierten Daten: Aufbewahrung der Zuordnungsdatei in einem getrennten System		Erstellung und Nutzung eines Berechtigungskonzepts
	Speicherung verschiedener Datenkategorien auf gesonderten Systemen oder Datenträgern		Festlegung von separaten Rechten für Datenbanksätze und -felder
	Trennung von Produktiv- und Testsystem		Weitere: _____
	Weitere: _____		

9. Bewertung der Wirksamkeit der Maßnahmen

Maßnahmen, die gewährleisten, dass die Wirksamkeit der vorgenannten technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüft, bewertet und evaluiert werden.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Weitere: _____		Regelmäßige Bewertung, ob die eingesetzte IT noch dem aktuellen Sicherheitsstand entspricht
			Regelmäßige Bewertung, ob die Richtlinien noch aktuell sind und angewendet werden
			Regelmäßige Schulung der Mitarbeiter
			Verantwortlicher und DSB setzen Anforderungen der DSGVO / BDSG dokumentiert um
			Zertifiziertes Datenschutzmanagement (z.B. VDS 10010) liegt vor
			Zertifiziertes Informationssicherheitsmanagement (z.B. ISO/IEC 27001, VDS 10000) liegt vor
			Weitere: _____

Der Verantwortliche bestätigt mit nachfolgender Unterschrift, dass die genannten technisch-organisatorischen Maßnahmen vorhanden und umgesetzt sind.

Name Firma: _____

Name Verantwortlicher (Klartext): _____

Ort, Datum, Unterschrift Verantwortlicher: _____

besondere Relevanz bei mobilem Arbeiten