Fragebogen zur

Anlage zu Art. 32 DSGVO

Technisch-organisatorische Maßnahmen

Unternehmen:

Nr.	Datensicherungsmaßnahmen des Autragnehmers	ja	nein	Bemerkungen ggf. Ansprechpartner
1.	**Vertraulichkeit** (Art. 32 Abs. 1 lit. B DSGVO)			
	1.0 Zutrittskontrolle Kein unbefugter Zugriff zu Datenverarbeitungsanlagen			
	1.0.1 Besitzen Sie elektrische Türöffner ?	☐	☐	
	1.0.2 Ist die Schlüsselvergabe in Ihrem Unternehmen geregelt ?	☐	☐	
	1.0.3 Haben Sie ein Zutrittskontrollsystem mit Magnet- oder Chipkarten ?	☐	☐	
	1.0.4 Gibt es bei Ihnen Pförtner bzw. einen Werkschutz ?	☐	☐	
	1.0.5 Werden Alarm und Videoanlagen eingesetzt ?	☐	☐	
	1.1 Zugangskontrolle Keine unbefugte Systembenutzung			
	1.1.1 Werden bei Ihnen Anforderungen an die Passwörter, z.B. Sicherheit, Länge, Sonderzeichen, regelmäßiger Wechsel gestellt ?	☐	☐	
	1.1.2 Setzen Sie in Ihrem Unternehmen Zwei-Faktor-Authentifizierung ein z.B. Hardware-Token und Kennwort /PIN ?	☐	☐	
	1.1.3 Werden bei Ihnen automatische Sperr-mechanismen eingesetzt z.B. Bildschirmschoner ?	☐	☐	
	1.1.4 Sind alle zugänglichen Datenträger mit personenbezogenen Daten verschlüsselt)	☐	☐	
	1.2 Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems			
	1.2.1 Ist in Ihrem Unternehmen ein Berechti-gungskonzept mit differenzierten Rollen, Transaktionen und Objekten etabliert ?	☐	☐	

1.2.2 Wird das Need-to-know-Prinzip (bedarfsgerecht) bei der Vergabe der Zugriffsrechte eingehalten ? ☐ ☐

1.2.3 Können die Zugriffsrechte ausgewertet werden ? ☐ ☐

1.2.4 Werden die einzelnen Zugriffe, sei es Kenntnisnahme, Veränderung oder Löschung, protokolliert ? ☐ ☐

1.3 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

1.3.1 Werden personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet ? ☐ ☐

1.3.2 Besitzt Ihr Berechtigungssystem Mandantenfähigkeit ? ☐ ☐

1.3.3 Verfügen Sie über ein Test- und ein Produktionssystem z.B. Sandboxing ? ☐ ☐

1.4 Pseudonymisierung

(Art 32 Abs. lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

1.4.1 Erfolgt die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen ? ☐ ☐

2. Integrität

(Art.32 Abs. 1 it b. DSGVO)

2.0 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

2.0.1 Wird jede elektronische Datenübertragung personenbezogener Daten verschlüsselt ? ☐ ☐

2.0.2 Werden Maßnahmen zur Absicherung des Transports von Datenträgern, z.B. Verschlüsselung mobiler Datenträger getroffen ? ☐ ☐

2.0.3 Werden elektronische Signaturen eingesetzt ? ☐ ☐

2.0.4 Werden virtuelle private Netzwerke (VPN) eingesetzt ? ☐ ☐

2.0.5 Setzen Sie Protokollierungssysteme ein, die die Weitergabe von Daten überwachen ? ☐ ☐

2.1 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

2.1.1 Werden alle Dateneingaben-, veränderungen und -löschungen protokolliert und ausgewertet ? ☐ ☐

2.1.2 Verfügen Sie über einen Administrator-Log ? ☐ ☐

2.1.3 Werden Dokumenten-Management-Systeme eingesetzt ? ☐ ☐

3. Verfügbarkeit und Belastbarkeit

(Art. 32 Abs. 1 lit

3.0 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

3.0.1 Haben Sie eine Backup-Strategie (online/offline; on-site/off-site) ? ☐ ☐

3.0.2 Besitzt Ihr Unternehmen eine unterbrechungsfreie Stromversorgung (USV) ? ☐ ☐

3.0.3 Setzen Sie Virenschutz und Firewall ein ? ☐ ☐

3.0.4 Wurde ein Notfallplan und entsprechende Meldewege etabliert ? ☐ ☐

3.0.5 Wird eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit c DSGVO) sichergestellt ? ☐ ☐

4. Verfahren zur regwelmäßigen Überprüfung,
Bewertung und Evaluierung
(Art. 32 Abs 1 lit dDSGVO; Art. 25 Abs. 1 DSGVO)

4.0 Auftragskontrolle
Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers

4.0.1	Werden alle Maßnahmen zur weisungsgemäßen Auftragsdatenverarbeitung getroffen und entsprechen diese der aktuellen Gesetzeslage ?	☐	☐
4.0.2	Wird ein formalisiertes Auftragsmanagement eingesetzt?	☐	☐

4.1 Datenschutz-Management ☐ ☐
Wird die Rechenschaftspflicht zum Nachweis der Einhaltung der gesetzlichen Grundsätze und Regelungen des Stands der Technik und Maßnahmen durch ein Datenschutz-Management-System sichergestellt ?

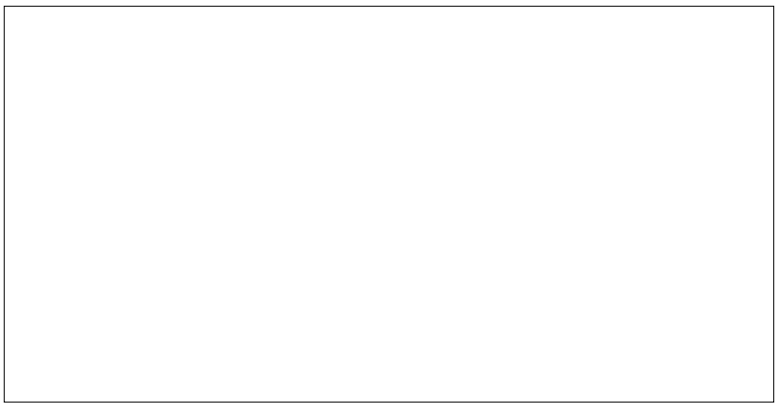
4.2 Incident-Response-Management ☐ ☐
Wird durch organisatorische und technische Maßnahmen / Prozesse sichergestellt, dass erkannte oder vermutete Sicherheitsvorfälle / Angriffe auf die IT-Infrastruktur bzw. Störungen (technische Probleme, Schwachstellen) erkannt und beseitigt werden können ?

4.3 Datenschutz-Management (Art. 25 Abs. 2 DSGVO) ☐ ☐
Wird durch geeignete technische und organisatorische Maßnahmen sichergestellt, dass in Bezug auf die Menge, den Umfang, der Speicherfrist und der Zugänglichkeit durch Voreinstellungen die Verarbeitung nur für den jeweiligen bestimmten Verarbeitungszweck erfolgen ?

Die Richtigkeit der gemachten Angaben wird bestätigt.

_____
Datum, Ort und Unterschrift

Funktion des Unterzeichners im Unternehmen:



Auftragnehmer / Firma

Ort, Datum Unterschrift