

Übersicht über die technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit

Dieser Anhang beschreibt die Anforderungen an die technischen und organisatorischen Maßnahmen, welche nach Art. 32 DSGVO für die Auftragsverarbeitung zu erfüllen sind.

Nachstehend sind die an den Auftragsverarbeiter gestellten Dokumentationspflichten aufgeführt, die spätestens beim Vorlegen des finalen Angebotes der Auftraggeberin einzureichen sind:

- Datenschutzkonzept (siehe C1)*
- Informationssicherheitskonzept**
- Angaben zu geeigneten Nachweisen im Kontext Informationssicherheit und Datenschutz, sofern vorliegend (siehe C2)

*nach Baustein CON.2 des BSI-Grundschutzkataloges

**nach BSI-Grundschutzkatalog oder ISO27001

C.1 Angaben zu umgesetzten Maßnahmen im Datenschutzkonzept

Es wird eine detaillierte und prüffähige Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen (TOM) im Datenschutzkonzept (DS-Konzept) gefordert. Im DSK muss auf folgende Gewährleistungsziele (einschließlich der beispielhaft aufgelisteten TOM) eingegangen werden:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
kein unbefugter Zutritt zu Datenverarbeitungsanlagen,
z. B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen
- Zugangskontrolle
keine unbefugte Systembenutzung,
z. B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- Zugriffskontrolle
kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems,
z. B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Trennungskontrolle
getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden,
z. B. Mandantenfähigkeit, Sandboxing
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
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.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport,
z. B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind,
z. B. Protokollierung, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust,
z. B. Backup-Strategie
- (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO).

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

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle

C.2 Angaben zu geeigneten Nachweisen im Kontext Informationssicherheit und Datenschutz

Zertifikate und sonstige geeignete Nachweise	Beschreibung
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
	Gültigkeit Nachweis Von: 01.01.2025 Bis: 01.01.2025
	Sind alle Standorte aus Anhang B - Geschäftsstandorte zertifiziert? Klicken oder tippen Sie hier, um Text einzugeben. Wird Zugang zum Zertifizierungs-/Prüfbericht gewährt? Klicken oder tippen Sie hier, um Text einzugeben.
	Sonstige Anmerkungen, insofern der Nachweis nicht alle Datenverarbeitungsstandorte abdeckt: Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
	Gültigkeit Nachweis Von: 01.01.2025 Bis: 01.01.2025
	Sind alle Standorte aus Anhang B - Geschäftsstandorte zertifiziert? Klicken oder tippen Sie hier, um Text einzugeben. Wird Zugang zum Zertifizierungs-/Prüfbericht gewährt? Klicken oder tippen Sie hier, um Text einzugeben.
	Sonstige Anmerkungen, insofern der Nachweis nicht alle Datenverarbeitungsstandorte abdeckt: Klicken oder tippen Sie hier, um Text einzugeben.
...	...

Ort, Datum: Klicken oder tippen Sie hier, um Text einzugeben.

Name des Erklärenden: Klicken oder tippen Sie hier, um Text einzugeben.