

Anlage zur IT-Sicherheit – Mindestanforderungen			
Nr.	Anforderung	Kategorie	Verweis
1	Verarbeitung, Speicherung und administrativer Zugriff (einschließlich Support/Fernwartung) ausschließlich in der EU/im EWR. Kein Zugriff aus Drittstaaten.	Muss	BSI OPS.2.3; Art. 44 ff. DSGVO; LV 4.1–4.5
2	Festplattenverschlüsselung aller Endgeräte nach Stand der Technik (z. B. BitLocker, AES-256) unter Nutzung des vorhandenen TPM.	Muss	BSI SYS.1.1, SYS.2.1; LV 1.1, 1.2
3	Hardware-Verschlüsselung des mobilen Sicherungsmediums (externe SSD).	Muss	BSI CON.3; LV 1.4
4	Verschlüsselte Ablage auf dem Netzwerkspeicher (NAS) und Berechtigungskonzept mit personalisierten Konten (keine geteilten Zugänge).	Muss	BSI SYS.1.8, ORP.4; LV 1.5
5	Datensicherungskonzept mit einem nicht dauerhaft verbundenen Sicherungsmedium (offline bzw. rotierend) gegen Ransomware; dokumentierter Wiederherstellungstest.	Muss	BSI CON.3; LV 1.3, 1.4, 4.6
6	Patch- und Schwachstellenmanagement: benannte Verantwortlichkeiten und Frist (SLA) für sicherheitskritische Updates (Betriebssysteme, Praxissoftware, TI-Komponenten, Firmware).	Muss	BSI OPS.1.1.3; LV 4.1, 4.2
7	Verschlüsselung der Datenübertragung (in transit) und ruhender Daten (at rest) nach Stand der Technik.	Muss	BSI CON.1
8	Fernwartung nur über gesicherten Zugang mit Zwei-Faktor-Authentifizierung (MFA); Verbindungsaufbau durch bzw. mit Freigabe des Auftraggebers; Protokollierung der Zugriffe; Speicherung der Protokolle in der EU/im EWR.	Muss	BSI OPS.2.3; Anlage 4 (Teleservice)
9	Protokollierung sicherheitsrelevanter Ereignisse (z. B. fehlgeschlagene Anmeldungen, Konfigurationsänderungen) und Einbindung in das Monitoring.	Muss	BSI OPS.1.1.5; LV 4.4
10	Meldung von Sicherheitsvorfällen an den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis.	Muss	BSI DER.2.1
11	Verpflichtung des eingesetzten Personals des Auftragnehmers zur Vertraulichkeit/Verschwiegenheit.	Muss	Vertrag 12.1
12	Exit- und Löschkonzept zum Vertragsende: Rückgabe der Daten in nutzbarem Format sowie nachweisliche, BSI-konforme Löschung/Vernichtung der Datenträger (Vernichtungsnachweis); gilt auch für Kopien beim Auftragnehmer/Subunternehmer.	Muss	BSI CON.6; Vertrag 12.5
13	Nachweis eines Informationssicherheits-Niveaus (z. B. Zertifikat ISO 27001 oder BSI IT-Grundschutz oder gleichwertig); Prüf-/Auditrecht des Auftraggebers.	Soll	BSI ORP.5

Hinweis:

– „Muss“ sind Mindestanforderungen; sie sind verbindlich und gegenüber den Bietern durchsetzbar.