Landkreis Anhalt-Bitterfeld

Anlage 1 – technisch und organisatorische Maßnahmen

Pseudonymisierung: *(Art. 32 Abs. 1 lit. a DSGVO)*	
Beispiele sind: • *Trennung von Kundenstammdaten und Kundenumsatzdaten* • *Trennung von Patienten-Kontaktdaten und Behandlungsdaten/Befunden etc.* • *Verwendung von Personal-, Kunden-, Patienten-Kennziffern statt Namen*	*auszufüllen durch den Auftragnehmer*
Verschlüsselung *(Art. 32 Abs. 1 lit. a DSGVO)*	
z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport. Beispiels sind symmetrische Verschlüsselung und asymmetrische Verschlüsselung	*auszufüllen durch den Auftragnehmer*
Gewährleistung der Vertraulichkeit der Systeme und Dienste *(Art. 32 Abs. 1 lit. b DSGVO)* *Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Es soll der unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindert werden, beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder Dritten.*	
Dazu zählen u.a. Maßnahmen zur: • *Zutrittskontrolle* • *Zugangskontrolle* • *Zugriffskontrolle* • *Weitergabekontrolle* • *Trennungskontrolle*	*auszufüllen durch den Auftragnehmer*

Gewährleistung der Integrität *(Art. 32 Abs. 1 lit. b DSGVO)* *Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren. Kurz, personenbezogene Daten dürfen nicht (unbemerkt) geändert werden können.*	
Beispiele sind Maßnahmen zur: • *Eingabekontrolle* • *organisatorische und technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokoll-Auswertungen/Revision,…*	*auszufüllen durch den Auftragnehmer*
Gewährleistung der Verfügbarkeit *(Art. 32 Abs. 1 lit. b DSGVO)* *Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.* *Personenbezogene Daten sollen dauernd und uneingeschränkt verfügbar sein und insbesondere vorhanden sein, wenn sie gebraucht werden.*	
Beispiele sind Maßnahmen zur: • *Verfügbarkeitskontrolle* • *Auftragskontrolle*	*auszufüllen durch den Auftragnehmer*
Gewährleistung der Belastbarkeit der Systeme *(Art. 32 Abs. 1 lit. b DSGVO)* *Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu im Auftrag verarbeiteten Daten aufgrund von Systemüberlastungen oder –abstürzen ist zu reduzieren. Das bedeutet, Systeme und Dienste sind so auszulegen, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben*	
Maßnahmen beziehen sich insbes. auf Speicher-, Zugriffs- und Leitungskapazitäten	*auszufüllen durch den Auftragnehmer*

Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall *(Art. 32 Abs. 1 lit. c DSGVO)* *Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.*	
Beispiele für Maßnahmen: • *Backup-Konzept* • *Redundante Datenspeicherung* • *Einsatz von Cloud-Services* • *Doppelte IT-Infrastruktur* • *Schatten-Rechenzentrum*	*auszufüllen durch den Auftragnehmer*
Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen *(Art. 32 Abs. 1 lit. d DSGVO)* *Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.*	
Beispiele: • *Entwicklung eines Sicherheitskonzepts* • *Prüfungen des DSB, der IT-Revision* • *Externe Prüfungen, Audits, Zertifizierungen*	*auszufüllen durch den Auftragnehmer*