Anlage 2 – Technische und organisatorische Maßnahmen

„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,...“		
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)		
Zutrittskontrolle	*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*	✓ Absicherung von Gebäudeschächten ✓ Automatisches Zugangskontrollsystem ✓ Manuelles Schließsystem ✓ Lichtschranken / Bewegungsmelder ✓ Sicherheitsschlösser ✓ Schlüsselregelung (Schlüsselausgabe etc.) ✓ Personenkontrolle beim Empfang ✓ Sorgfältige Auswahl von Reinigungspersonal
Zugangskontrolle	*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*	✓ Zuordnung von Benutzerrechten ✓ Erstellen von Benutzerprofilen ✓ Passwortvergabe ✓ automatische Sperrmechanismen ✓ Authentifikation mit Benutzername / Passwort ✓ Zuordnung von Benutzerprofilen zu IT-Systemen ✓ Gehäuseverriegelungen ✓ Einsatz von VPN-Technologie ✓ Einsatz von Anti-Viren-Software ✓ Einsatz einer Hardware-Firewall ✓ Einsatz einer Software-Firewall
Zugriffskontrolle	*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*	✓ Identifizierungs- und Authentifizierungssystem ✓ Erstellen eines Berechtigungskonzepts ✓ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten ✓ Verschlüsselungsverfahren/-systeme ✓ Vier-Augen-Prinzip bei Spezialan-

		wendungen ✓ Sichere Aufbewahrung von Datenträgern (Datentresor) ✓ Verschlüsselung von Datenträgern ✓ physische Löschung von Datenträgern vor Wiederverwendung ✓ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399) ✓ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) ✓ Protokollierung (der Vernichtung) zum Nachvollzug
Trennungskontrolle	*Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist zu garantieren!*	✓ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern ✓ Logische Mandantentrennung (softwareseitig) ✓ Rechteverwaltung bzw. Erstellung eines Berechtigungskonzepts ✓ Festlegung von Datenbankrechten ✓ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden ✓ Versehen der Datensätze mit Zweckattributen/Datenfeldern ✓ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System ✓ Trennung von Produktiv- und Testsystem ✓ Sandboxing ✓ Protokollierung und Beweissicherung
Pseudonymisierung	*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 entsprechende technischen und organisatorischen Maßnahmen unterliegen.*	

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

Weitergabekontrolle	*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*	✓ Einrichtungen von Standleitungen bzw. VPN-Tunneln ✓ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form ✓ Regelung / Dokumentation Ausgabe- und Empfängerkreis ✓ Fernwartungskonzept ✓ Beim physischen Transport: sichere Transportbehälter/-verpackungen
Eingabekontrolle	*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*	✓ Identifizierung und Authentifizierung ✓ Dokumentenmanagement ✓ Protokollierung der Eingabe, Änderung und Löschung von Daten ✓ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. ✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) ✓ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)		
Verfügbarkeitskontrolle	*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind*	✓ Virenschutz ✓ Firewall / IDS ✓ Unterbrechungsfreie Stromversorgung (USV) ✓ Klimaanlage in Serverräumen ✓ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen ✓ Schutzsteckdosenleisten in Serverräumen ✓ Feuer- und Rauchmeldeanlagen ✓ Feuerlöschgeräte in Server-

		räumen ✓ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen ✓ Backup-Strategie (online/offline; on-site/off-site) ✓ Verfügbarkeit eines Notfall-RZ ✓ Erstellen eines Backup- und Recovery-Konzepts ✓ Testen von Datenwiederherstellung ✓ Erstellen eines Notfallkonzeptes / Notfallplans ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort ✓ Serverräume nicht unter sanitären Anlagen
Wiederherstellbarkeit	*Maßnahmen, die die rasche Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust oder Beschädigung gewährleisten.* Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)	✓ Backup-Strategie (online/offline; on-site/off-site) ✓ Verfügbarkeit eines Notfall-RZ ✓ Erstellen eines Backup- und Recovery-Konzepts ✓ Testen von Datenwiederherstellung ✓ Erstellen eines Notfallkonzeptes / Notfallplans ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

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		
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)	*Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.* *Data Privacy by Design and by Default*	✓ Pseudonymisierung ✓ Beschränkung bzgl. der Menge der erhobenen Auftragsdaten ✓ Beschränkung des Umfangs der Verarbeitung der erhobenen Daten ✓ Beschränkung der Speicherfrist ✓ Beschränkung der Zugänglichkeit
Auftragskontrolle	*Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeitet werden (können)!*	✓ Eindeutige Vertragsgestaltung / vertragliche Regelungen ✓ Formalisiertes Auftragsmanagement

		✓ Strenge Auswahl des Dienstleisters (insbesondere hinsichtlich Datensicherheit) ✓ Vorabüberzeugungspflicht ✓ Vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen ✓ Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG ✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG) ✓ Auftragnehmer hat Datenschutzbeauftragten bestellt ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags ✓ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart ✓ Vertragsstrafen bei Verstößen

Geprüft durch Keyed GmbH in Frankfurt am 14.05.2018.
Auditor: Nils Möllers