Technische und organisatorische Maßnahmen der Firma Datentechnik Blum GmbH

Stand: Mai 2018

„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.*	Typische Maßnahmen sind z.B.: ☒ Alarmanlage ☒ Absicherung von Gebäudeschächten ☒ Manuelles Schließsystem ☒ Sicherheitsschlösser
Zugangskontrolle	*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*	Typische Maßnahmen sind z.B.: ☒ Zuordnung von Benutzerrechten ☒ Passwortvergabe ☒ automatische Sperrmechanismen ☒ Authentifikation mit Benutzername / Passwort ☒ Einsatz von VPN-Technologie ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) ☒ Einsatz von Anti-Viren-Software ☒ Einsatz einer Software-Firewall ☒ Einsatz von Intrusion-Detection-Systemen Sonstiges: _____
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.*	Typische Maßnahmen sind z.B.: ☒ Identifizierungs- und Authentifizierungssystem ☒ Erstellen eines Berechtigungskonzepts ☒ Verwaltung der Rechte durch Systemadministrator ☒ Anzahl der Administratoren auf das „Notwendigste „ reduziert ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten ☒ Sichere Aufbewahrung von Datenträgern (Datentresor) ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel ☒ Löschung von Datenträgern vor Wiederverwendung ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern
Trennungskontrolle	*Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist zu garantieren!*	Typische Maßnahmen sind z.B.: ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

		☒ Logische Mandantentrennung (softwareseitig) ☒ Rechteverwaltung bzw. Erstellung eines Berechtigungskonzept ☒ Festlegung von Datenbankrechten ☒ Versehen der Datensätze mit Zweckattributen/Datenfeldern ☒ Trennung von Produktiv- und Testsystem
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.*	Typische Maßnahmen sind z.B.: ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln ☒ E-Mail Verschlüsselung ☒ Verschlüsselung des Datencontainers ☒ Regelung / Dokumentation Ausgabe- und Empfängerkreis ☒ 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.*	Typische Maßnahmen sind z.B.: ☒ 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.

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*	Typische Maßnahmen sind z.B.: ☒ Virenschutz ☒ Firewall / IDS ☒ Unterbrechungsfreie Stromversorgung (USV) ☒ Schutzsteckdosenleisten in Serverräumen ☒ Feuer- und Rauchmeldeanlagen ☒ Erstellen eines Backup- und Recovery-Konzepts

		☒ Testen von Datenwiederherstellung ☒ Erstellen eines Notfallkonzeptes / Notfallplans ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
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)*	Typische Maßnahmen sind z.B.: ☒ 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*	☒ Beschränkung des Umfangs der Verarbeitung der erhobenen Daten
Auftragskontrolle	*Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeitet werden (können)!*	☒ Eindeutige Vertragsgestaltung / vertragliche Regelungen ☒ Strenge Auswahl des Dienstleisters (insbesondere hinsichtlich Datensicherheit) ☒ 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) ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Datentechnik Blum GmbH
Steinweg 5
35327 Ulrichstein
Tel. 0 66 45 / 91 91 91
Fax 0 66 45 / 6 71 (91 91 99)

Ulrichstein, 21.05.2018

(Ort, Datum) (Unterschrift)