Anlage Datenschutzkonzept gemäß Art. 32 DSGVO:

Maßnahme	Umsetzung
M.1 Maßnahmen zur Vertraulichkeit **Datenzentren** Brief365 besitzt, mietet oder betreibt keine Brief365 Server-Infrastruktur für seine Büros oder Produktionsumgebung. Die Brief365-Unternehmensumgebung ist eine rein cloud-basierte Infrastruktur, die in Rechenzentren in Deutschland untergebracht ist, welche durch Drittanbieter betriebenen werden. Die TOMs der STACKIT finden Sie hier.	
Brief365 verfügt über Zugangskontrollmaßnahmen, die den unbefugten Zutritt zu Datenverarbeitungsanlagen verhindern sollen, in denen personenbezogene Daten gespeichert oder verarbeitet werden.	
M.1.1 Beschreibung der Zutrittskontrolle:	- Absicherung von Gebäudeschächten - Sicherheitsschlösser - Personenkontrolle - Schlüsselregelung
M.1.2 Beschreibung der Zugangskontrolle:	- Authentifikation mit Benutzer und Passwort - Authentifikation mit biometrischen Daten - Einsatz von Anti-Viren-Software - Einsatz von Firewalls - Verschlüsselung von Datenträgern - Verschlüsselung von Smartphones - Kennwortverfahren (Sonderzeichen, Wechsel) - Automatische Sperrung (Pausenschaltung) - Sperrung des Zugangs bei Fehlversuchen - Zwei-Faktor-Authentifizierung - Benutzerberechtigungen verwalten - Erstellen von Benutzerprofilen - Passwortvergabe/Passwortregeln - Personenkontrolle - Schlüsselregelung
M.1.3 Beschreibung der Zugriffskontrolle:	- Einsatz von Aktenvernichtern - Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399) - Physische Löschung von Datenträgern vor deren Wiederverwendung - Protokollierung von Zugriffe auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten - Verschlüsselung von Datenträgern - Verschlüsselung von Smartphones - Anzahl der Administratoren auf das Notwendigste reduzieren - Erstellung eines Berechtigungskonzepts (Rollen) - Passwortrichtlinie inkl. Länge und Wechsel - Sichere Aufbewahrung von Datenträgern - Verwaltung der Benutzerrechte durch Systemadministratoren - Verbot/Regelung für den Einsatz privater Datenträger

M.1.4 Beschreibung der Weitergabekontrolle:	- E-Mail-Verschlüsselung - Elektronische Signatur - Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen - Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen - Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
M.1.5 Beschreibung des Trennungsgebots:	- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten abgesicherten IT-System - Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern - Trennung von Produktiv- und Testsystem - Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden - Erstellung eines Berechtigungskonzepts - Festlegung von Datenbankrechten - Logische Mandantentrennung (softwareseitig)
M.2 Maßnahmen zur Integrität	
M.2.1 Beschreibung der Eingabekontrolle:	- Protokollierung der Eingabe, Änderung und Löschung von Daten - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind - Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit	
M.3.1 Beschreibung der Verfügbarkeitskontrolle:	- Feuerlöschgeräte in Serverräumen - Feuer- und Rauchmeldeanlagen - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen - Klimaanlage in Serverräumen - Schutzsteckdosenleisten in Serverräumen - Unterbrechungsfreie Stromversorgung (USV) - Backup-Verfahren - Alarmmeldung bei unberechtigten Zutritten zu Serverräumen - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort - Erstellen eines Backup- und Recoverykonzepts - Erstellen eines Notfallplans - Testen der Datenwiederherstellung - Serverräume nicht unter sanitären Anlagen

M.4 Weitere Maßnahmen zum Datenschutz	
M.4.1 Beschreibung der Auftragskontrolle:	- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten - Schriftliche Weisungen an den Auftragnehmer (AV-Vertrag) - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis - Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation - Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren - Definierte Vorgehensweise der Vertragsbeendigung
M.4.2 Beschreibung des Managementsystems zum Datenschutz:	- Durchführung regelmäßiger interner Audits - Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen - Managementsystem zum Datenschutz - Richtlinie für die Bearbeitung von Anfragen von Betroffenen unter der DS-GVO

Anlage Subunternehmer:

Subunternehmer	Anschrift	Auftragsbeschreibung
regiocom SE	Marienstraße 1, 39112 Magdeburg	DevOps
STACKIT - Lidl/Schwarz Gruppe (Schwarz IT KG) ab Mai 2024	Stiftsbergstraße 1, 74172 Neckarsulm	IT-/TK-Dienstleistungen (Cloud, Rechenzentrum)
Paragon Customer Communications Weingarten GmbH	Josef Bayer Straße 5, 88250 Weingarten	Drucken, Kuvertieren, Versandbereitstellung
Pipedrive OÜ	Mustamäe tee 3a, 10615 Tallinn, Estland	CRM-Software
Myra Security GmbH (freiwillige Aufnahme gem. 7 (8) des AVV)	Landsberger Straße 187, 80687 München	Firewall