Technische und organisatorische Maßnahmen

Anlage zur Auftragsverarbeitungsvereinbarung | Art. 32 DSGVO

1. Geltungsbereich

Diese Anlage beschreibt die wesentlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten, die im Auftrag der Kunden in meinOnlineBüro verarbeitet werden. Die Maßnahmen orientieren sich an Art. 32 DSGVO und dem jeweiligen Schutzbedarf.

2. Zutritts- und physische Sicherheit

Die produktiven Hosting- und Infrastrukturleistungen werden über externe Rechenzentrumsdienstleister erbracht. Die physische Absicherung der Rechenzentrumsbereiche einschließlich Zutrittskontrollen und infrastruktureller Schutzmaßnahmen liegt im jeweiligen Verantwortungsbereich dieser Dienstleister.

3. Zugangs- und Berechtigungskontrolle

Die Anwendung verwendet passwortgeschützte Zugänge. Administrations- und Benutzerberechtigungen werden entsprechend den jeweiligen Aufgaben und Zuständigkeiten vergeben. Der Auftraggeber verwaltet die fachlichen Benutzerrechte innerhalb der von der Anwendung bereitgestellten Funktionen. Technische Administrationszugänge sind auf berechtigte Personen beschränkt.

4. Zugriffsschutz und Vertraulichkeit

Der Zugriff auf Kundendaten ist auf berechtigte Vorgänge und Personen begrenzt. Die mit der Verarbeitung betrauten Personen werden zur Vertraulichkeit verpflichtet. Netzwerk- und Systemzugriffe werden durch geeignete technische Schutzmechanismen begrenzt.

5. Übertragung und Kommunikationssicherheit

Für den Zugriff auf die webbasierte Anwendung werden verschlüsselte Verbindungen eingesetzt. Bei der Integration externer E-Mail-Postfächer werden die vom jeweiligen E-Mail-Dienst und der Anwendung unterstützten sicheren Verbindungs- und Authentisierungsverfahren verwendet.

6. Mandantentrennung und Datenintegrität

Kundendaten werden in der Anwendung logisch voneinander getrennt verarbeitet. Berechtigungen begrenzen den Zugriff auf die jeweils zugeordneten Daten. Die Verarbeitung erfolgt innerhalb der für die jeweiligen Funktionen vorgesehenen technischen Abläufe.

7. E-Mail-Integration und CRM

Die Original-E-Mails und Anhänge verbleiben grundsätzlich beim jeweiligen Postfachanbieter des Kunden. Der Kunde kann eine Kopie des E-Mail-Textes ohne Anhänge sowie einen Verweis auf die Original-E-Mail in seiner CRM-Kontakthistorie ablegen. Diese gespeicherten Textkopien unterliegen den Schutzmaßnahmen für sonstige CRM-Kundendaten.

8. Verfügbarkeit und Datensicherung

Für die bereitgestellten Systeme werden Datensicherungs- und Wiederherstellungsverfahren im Zusammenwirken mit den eingesetzten Hosting-Dienstleistern genutzt. Der Betrieb umfasst technische Maßnahmen zur Aufrechterhaltung der Verfügbarkeit und zur Behandlung von Störungen.

9. Sicherheitswartung und Vorfälle

Die für den Betrieb verantwortlichen Stellen führen technische Wartungs- und Sicherheitsmaßnahmen entsprechend ihren Zuständigkeiten durch. Datenschutz- und Sicherheitsvorfälle werden bewertet und bei Betroffenheit von Auftragsdaten nach den vertraglichen und gesetzlichen Vorgaben behandelt.

10. Überprüfung und Weiterentwicklung

Die technischen und organisatorischen Maßnahmen werden unter Berücksichtigung der Risiken und der technischen Entwicklung angepasst. Änderungen dürfen das insgesamt erforderliche Schutzniveau nicht unangemessen herabsetzen.