Vereinbarung zur Auftragsverarbeitung für eMailButler24

Vereinbarung nach Artikel 28 Datenschutz Grundverordnung einschließlich Anlagen

Dokumentstatus	Allgemeingültiger B2B-Vertragsentwurf - offene Angaben türkis markiert
Version	1.0
Stand	18. September 2026

Diese allgemeingültige Vereinbarung regelt die Verarbeitung personenbezogener Daten durch den Anbieter im Auftrag des im Bestellprozess bezeichneten Geschäftskunden bei der Nutzung von eMailButler24. Sie wird über eine gesonderte Pflicht-Checkbox elektronisch abgeschlossen. Eine handschriftliche Unterschrift ist nicht erforderlich.

[VOR VERÖFFENTLICHUNG ERGÄNZEN UND PRÜFEN] Die türkis markierten Anbieter- und Kontaktdaten, die tatsächlichen technischen und organisatorischen Maßnahmen sowie sämtliche Unterauftragnehmer, Verarbeitungsorte und Transfergrundlagen müssen vor Veröffentlichung vollständig und technisch zutreffend eingetragen werden.

Auftragsverarbeiter	Verantwortlicher
[ANBIETERFIRMA UND RECHTSFORM]	Kunde gemäß Bestellprozess oder Bestellbestätigung
[VOLLSTÄNDIGE ANSCHRIFT]	Vollständige Unternehmensanschrift gemäß Bestellung
[REGISTERGERICHT UND REGISTERNUMMER]	Registerdaten, soweit angegeben oder erforderlich
[VERTRETUNGSBERECHTIGTE PERSON]	Im Bestellprozess handelnde, zum Abschluss berechtigte Person
[DATENSCHUTZKONTAKT UND VERTRAGSEMAIL]	Geschäftliche E-Mail-Adresse gemäß Bestellung

1 Gegenstand Geltung und Rangfolge

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen, soweit dies zur Bereitstellung von eMailButler24 erforderlich ist. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien.

Die Vereinbarung gilt für alle Tätigkeiten, bei denen Beschäftigte des Auftragsverarbeiters oder von ihm eingesetzte Unterauftragnehmer personenbezogene Daten des Verantwortlichen verarbeiten können. Die Einzelheiten ergeben sich aus Anlage 1.

Bei Widersprüchen gehen die Regelungen dieser Vereinbarung den Allgemeinen Geschäftsbedingungen und sonstigen Vertragsbestandteilen vor, soweit die Verarbeitung personenbezogener Daten betroffen ist. Zwingendes Datenschutzrecht bleibt unberührt.

2 Dauer der Verarbeitung

Die Vereinbarung beginnt mit der dokumentierten Bestätigung der AVV-Checkbox durch den Kunden und muss spätestens vor der ersten Verarbeitung personenbezogener Echtdaten abgeschlossen sein. Sie gilt für die Dauer des SaaS-Vertrags. Pflichten, die ihrem Zweck nach über das Vertragsende hinausreichen, bleiben bis zur vollständigen Löschung oder Rückgabe der Daten bestehen.

3 Art und Zweck der Verarbeitung

Der Auftragsverarbeiter betreibt eMailButler24 als KI-gestützten E-Mail-Assistenten. Die Verarbeitung dient insbesondere der Anbindung freigegebener Postfächer, dem Abruf ausgewählter Nachrichten und Metadaten, der Analyse von Kommunikationsinhalten, dem Abgleich mit freigegebenen Wissensquellen, der Erstellung von Antwortentwürfen sowie der Protokollierung sicherheits- und vertragsrelevanter Vorgänge.

Ein automatischer Versand oder eine selbstständige Bearbeitung von E-Mails ist nur Gegenstand der Verarbeitung, wenn diese Funktion ausdrücklich vereinbart, technisch aktiviert und in der Weisung des Verantwortlichen abgebildet wurde.

Der Auftragsverarbeiter verarbeitet die Daten nicht für eigene Werbezwecke und verwendet sie nicht zum Training allgemein verfügbarer KI-Modelle. Eine weitergehende Produktentwicklung mit Kundendaten bedarf einer gesonderten, rechtlich tragfähigen Vereinbarung und ist nicht von diesem Vertrag umfasst.

4 Verantwortung und Weisungen

Der Verantwortliche bleibt für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Betroffenenrechte, die Auswahl der verarbeiteten Postfächer und Inhalte sowie die Erteilung zulässiger Weisungen verantwortlich.

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Als anfängliche Weisung gelten der SaaS-Vertrag, diese Vereinbarung, die vom Verantwortlichen vorgenommene Konfiguration und die bestimmungsgemäße Nutzung des Dienstes.

Zusätzliche Weisungen können über die vereinbarten Supportwege in Textform erteilt werden. Verursacht eine Weisung Aufwand, der nicht durch die vereinbarte Vergütung abgedeckt ist, informiert der Auftragsverarbeiter vor der Umsetzung über den voraussichtlichen Aufwand.

Hält der Auftragsverarbeiter eine Weisung für datenschutzwidrig, informiert er den Verantwortlichen unverzüglich und darf die Umsetzung bis zur Klärung aussetzen. Ist der Auftragsverarbeiter gesetzlich zu einer Verarbeitung verpflichtet, informiert er den Verantwortlichen vorab, soweit das Gesetz dies erlaubt.

5 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter stellt sicher, dass zur Verarbeitung befugte Personen nur im erforderlichen Umfang zugreifen und sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftragsverarbeiter ergreift die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen und passt sie unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art und des Umfangs der Verarbeitung sowie der Risiken angemessen an. Das vereinbarte Schutzniveau darf nicht unterschritten werden.

Der Auftragsverarbeiter führt ein Verzeichnis der im Auftrag durchgeführten Verarbeitungstätigkeiten, soweit dies gesetzlich erforderlich ist, und arbeitet auf Anfrage mit der zuständigen Aufsichtsbehörde zusammen.

Der Auftragsverarbeiter bestellt einen Datenschutzbeauftragten, soweit die gesetzlichen Voraussetzungen vorliegen, und teilt dem Verantwortlichen dessen Kontaktdaten mit. Andernfalls benennt er eine zuständige Datenschutzkontaktstelle.

Der Auftragsverarbeiter trennt Kundendaten logisch voneinander und verwendet keine produktiven Kundendaten in Entwicklungs- oder Testumgebungen, soweit sie nicht zuvor wirksam anonymisiert wurden oder der Verantwortliche dies ausdrücklich angewiesen hat.

6 Unterauftragnehmer

Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 3 aufgeführten Unterauftragnehmer. Der Auftragsverarbeiter verpflichtet jeden Unterauftragnehmer vertraglich mindestens zu denselben Datenschutzpflichten, die ihm nach dieser Vereinbarung obliegen.

Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Kalendertage vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragnehmers in Textform. Die Mitteilung enthält Name, Sitz, Tätigkeit, Verarbeitungsort und gegebenenfalls die Grundlage einer Drittlandübermittlung.

Der Verantwortliche kann innerhalb von 14 Kalendertagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Die Parteien suchen zunächst eine zumutbare Lösung. Ist keine Lösung möglich, kann der Verantwortliche den betroffenen Dienst zum Zeitpunkt der Änderung außerordentlich kündigen.

Hilfsleistungen ohne Zugriffsmöglichkeit auf personenbezogene Daten gelten nicht als Unterauftragsverarbeitung. Besteht bei Wartung, Support oder Entwicklung die Möglichkeit eines Zugriffs, wird der Dienstleister als Unterauftragnehmer behandelt.

7 Verarbeitungsorte und Drittlandübermittlungen

Die reguläre Speicherung und KI-Verarbeitung erfolgen an den in Anlage 3 genannten Orten. Eine Aussage, dass Daten Deutschland nicht verlassen, setzt voraus, dass auch Support, Administration, Backups, Protokollierung und sämtliche Unterauftragnehmer entsprechend beschränkt sind.

Eine Übermittlung in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur auf dokumentierte Weisung oder wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Soweit kein Angemessenheitsbeschluss besteht, werden geeignete Garantien, insbesondere anwendbare EU-Standardvertragsklauseln, sowie erforderliche ergänzende Maßnahmen vereinbart und dokumentiert.

Ein Fernzugriff aus einem Drittland gilt als Drittlandübermittlung, auch wenn Daten nur auf einem Bildschirm angezeigt und nicht dauerhaft gespeichert werden. Zugriffe aus den Vereinigten Arabischen

Emiraten dürfen daher nur erfolgen, wenn sie in Anlage 3 ausgewiesen, technisch begrenzt, protokolliert und rechtlich abgesichert sind.

8 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten bei der Erfüllung von Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.

Richtet eine betroffene Person einen Antrag unmittelbar an den Auftragsverarbeiter, leitet er ihn unverzüglich an den Verantwortlichen weiter und beantwortet ihn nicht selbst, sofern der Verantwortliche ihn nicht hierzu angewiesen hat.

Soweit die Unterstützung über die regulären Produktfunktionen und einen angemessenen Standardaufwand hinausgeht, darf der Auftragsverarbeiter den zusätzlichen Aufwand nach vorheriger Abstimmung berechnen. Dies gilt nicht, wenn die Unterstützung wegen eines vom Auftragsverarbeiter zu vertretenden Verstoßes erforderlich wird.

9 Datenschutzverletzungen und weitere Unterstützung

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, in der Regel innerhalb von 24 Stunden nach Bekanntwerden, über eine Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft.

Die Meldung enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten- und Personenkategorien, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen sowie eine Kontaktstelle. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung bei dessen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Sicherheitsbewertungen, Meldungen an Aufsichtsbehörden, Benachrichtigungen betroffener Personen und Datenschutz-Folgenabschätzungen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über behördliche Anfragen oder Kontrollmaßnahmen, soweit dies rechtlich zulässig ist und die Auftragsverarbeitung betrifft.

10 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieser Vereinbarung nachzuweisen. Geeignete aktuelle Prüfberichte, Zertifikate und dokumentierte Sicherheitsnachweise sollen vorrangig verwendet werden.

Der Verantwortliche darf einmal pro Kalenderjahr sowie zusätzlich bei konkretem Anlass eine Prüfung durchführen oder durch einen zur Vertraulichkeit verpflichteten unabhängigen Prüfer durchführen lassen. Prüfungen sind grundsätzlich mindestens 14 Arbeitstage vorher anzukündigen, während üblicher Geschäftszeiten durchzuführen und auf den erforderlichen Umfang zu beschränken.

Der Prüfer darf kein unmittelbarer Wettbewerber des Auftragsverarbeiters sein. Geschäftsgeheimnisse, Sicherheitsinteressen und Rechte anderer Kunden sind zu schützen. Der Verantwortliche trägt die angemessenen Kosten einer Prüfung, sofern sie nicht einen wesentlichen vom Auftragsverarbeiter zu vertretenden Verstoß bestätigt.

11 Rückgabe und Löschung

Während der Vertragslaufzeit kann der Verantwortliche exportierbare Daten über die bereitgestellten Funktionen abrufen. Nach Vertragsende löscht oder gibt der Auftragsverarbeiter die

personenbezogenen Daten nach Wahl des Verantwortlichen zurück, soweit keine gesetzliche Aufbewahrungspflicht besteht.

Produktive Daten werden spätestens 30 Kalendertage nach Vertragsende gelöscht. Sicherungskopien werden im Rahmen des regulären Backup-Zyklus spätestens nach 90 Kalendertagen überschrieben oder gelöscht. Bis dahin dürfen sie nur zur Wiederherstellung nach einem Sicherheits- oder Systemausfall verwendet werden.

Innerhalb des laufenden Betriebs werden für Antwortentwürfe verwendete E-Mail-Inhalte und Historien grundsätzlich höchstens 90 Tage gespeichert, sofern der Verantwortliche keine kürzere zulässige Frist konfiguriert. Sicherheits- und Audit-Protokolle werden grundsätzlich höchstens 12 Monate gespeichert. Abweichende Fristen müssen in Anlage 1 oder der Bestellung dokumentiert werden.

Der Auftragsverarbeiter bestätigt die Löschung auf begründete Anfrage in Textform. Gesetzlich aufzubewahrende Daten werden gesperrt und nach Ablauf der Aufbewahrungsfrist gelöscht.

12 Vertraulichkeit

Beide Parteien behandeln personenbezogene Daten, Sicherheitsinformationen, Geschäftsgeheimnisse und sonstige vertrauliche Informationen der jeweils anderen Partei vertraulich. Die Verpflichtung besteht nach Vertragsende fort.

Der Auftragsverarbeiter legt dem Verantwortlichen personenbezogene Daten nur offen, soweit dies zur Vertragserfüllung, aufgrund einer dokumentierten Weisung oder wegen einer gesetzlichen Verpflichtung erforderlich ist.

13 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO, den sonstigen zwingenden gesetzlichen Bestimmungen und den wirksam vereinbarten Haftungsregelungen des Hauptvertrags. Gesetzliche Ansprüche betroffener Personen werden durch diese Vereinbarung nicht eingeschränkt.

14 Elektronischer Abschluss und Schlussbestimmungen

Diese Vereinbarung wird elektronisch über eine gesonderte, nicht vorangekreuzte Pflicht-Checkbox abgeschlossen. Der Verantwortliche kann sie vor Vertragsschluss über einen eindeutig bezeichneten Link als PDF aufrufen, herunterladen und speichern. Der Auftragsverarbeiter protokolliert das bezeichnete Unternehmen, die handelnde Person, die geschäftliche E-Mail-Adresse, Datum und Uhrzeit sowie die akzeptierte AVV-Version und stellt mit der Auftragsbestätigung die akzeptierte Fassung oder einen dauerhaft verfügbaren Downloadlink bereit.

Änderungen dieser Vereinbarung bedürfen mindestens der Textform. Änderungen der Anlagen dürfen nach dem in dieser Vereinbarung vorgesehenen Verfahren erfolgen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

Sollte eine Bestimmung unwirksam sein, bleiben die übrigen Bestimmungen wirksam. An die Stelle der unwirksamen Bestimmung treten die gesetzlichen Vorschriften.

Anlage 1 Beschreibung der Verarbeitung

Die folgende Beschreibung konkretisiert Gegenstand, Umfang und Grenzen der Verarbeitung.

Merkmal	Beschreibung
Gegenstand	Bereitstellung von eMailButler24 als KI-gestützter E-Mail-Assistent im gewählten Tarif
Zwecke	Anbindung freigegebener Postfächer, Analyse ausgewählter E-Mails und Wissensquellen, Erzeugung von Antwortentwürfen, Bereitstellung von Verwaltungsfunktionen, Sicherheit und Fehleranalyse
Verarbeitungsvorgänge	Abrufen, Erfassen, Ordnen, Speichern, Auslesen, Abgleichen, Übermitteln an genehmigte KI-Dienste, Generieren, Bereitstellen, Protokollieren, Einschränken und Löschen
Dauer	Dauer des SaaS-Vertrags zuzüglich der in Ziffer 11 geregelten Lösch- und Backupfristen
Datenarten	Identitäts- und Kontaktdaten, E-Mail-Adressen, Kommunikationsinhalte, Signaturen, Metadaten, Unternehmens- und Vorgangsdaten, Benutzer- und Berechtigungsdaten, Audit- und Sicherheitsprotokolle, freigegebene Wissensdokumente
Besondere Daten	Besondere Kategorien personenbezogener Daten und Berufsgeheimnisse können in E-Mail-Inhalten zufällig enthalten sein. Der Verantwortliche prüft Erforderlichkeit und zusätzliche Schutzpflichten.
Betroffene Personen	Beschäftigte und Beauftragte des Verantwortlichen, Kunden, Interessenten, Lieferanten, Geschäftspartner, Bewerber sowie sonstige Absender und Empfänger der angebundenen Kommunikation
Speicherfristen	E-Mail-Historie grundsätzlich 90 Tage, Audit- und Sicherheitsprotokolle grundsätzlich 12 Monate, produktive Daten nach Vertragsende 30 Tage, Backups nach Vertragsende höchstens 90 Tage
Automatisierter Versand	Nicht umfasst, sofern nicht ausdrücklich bestellt, aktiviert und angewiesen

Anlage 2 Technische und organisatorische Maßnahmen

Die nachstehenden Maßnahmen bilden das vertraglich zugesagte Mindestniveau. Vor dem produktiven Einsatz ist technisch zu bestätigen, dass jede Maßnahme tatsächlich umgesetzt ist.

1 Organisation und Verantwortlichkeit

- Dokumentierte Zuständigkeiten für Betrieb, Informationssicherheit und Datenschutz
- Verpflichtung berechtigter Personen auf Vertraulichkeit und regelmäßige Sensibilisierung
- Dokumentiertes Verfahren für Sicherheitsvorfälle, Datenschutzverletzungen und Eskalationen
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen

2 Zugangs und Berechtigungsschutz

- Personenbezogene Benutzerkonten und rollenbasierte Berechtigungen nach dem Prinzip der geringsten Rechte
- Mehrfaktor-Authentifizierung für administrative und privilegierte Zugänge
- Regelmäßige Überprüfung und unverzüglicher Entzug nicht mehr benötigter Berechtigungen
- Zeitlich begrenzte und protokollierte Freigabe von Supportzugriffen

3 Verschlüsselung und Übertragung

- Verschlüsselte Datenübertragung mit aktuellen, als sicher anerkannten Transportprotokollen
- Verschlüsselung gespeicherter Daten und Sicherungskopien, soweit technisch verfügbar und risikoadäquat
- Sichere Verwaltung von Schlüsseln, Geheimnissen und Zugangstokens außerhalb des Quellcodes
- OAuth oder vergleichbare sichere Verfahren für unterstützte Postfachanbindungen, soweit verfügbar

4 Mandantentrennung und Datenminimierung

- Logische Trennung der Daten unterschiedlicher Kunden auf Anwendungs- und Datenbankebene
- Beschränkung auf die vom Verantwortlichen ausgewählten Postfächer, Ordner und Wissensquellen
- Keine Nutzung produktiver Kundendaten in Entwicklungs- und Testumgebungen ohne wirksame Anonymisierung oder ausdrückliche Weisung
- Keine Verwendung von Kundendaten zum Training allgemein verfügbarer KI-Modelle

5 Protokollierung und Kontrolle

- Protokollierung administrativer Zugriffe, sicherheitsrelevanter Änderungen und wesentlicher Verarbeitungsvorgänge
- Schutz der Protokolle vor unbefugter Änderung und Zugriffsbeschränkung
- Definierte Aufbewahrungsfrist von grundsätzlich höchstens 12 Monaten
- Regelmäßige Auswertung sicherheitsrelevanter Ereignisse nach Risiko und Anlass

6 Verfügbarkeit und Wiederherstellung

- Regelmäßige Sicherung betriebsrelevanter Daten mit getrennten Zugriffsrechten
- Dokumentierte Wiederherstellungsverfahren und regelmäßige Wiederherstellungstests
- Überwachung zentraler Dienste und geregelte Behandlung von Störungen
- Schutz vor Schadsoftware sowie zeitnahe Installation sicherheitsrelevanter Aktualisierungen

7 Löschung und Aufbewahrung

- Automatisierte oder dokumentierte Löschung entsprechend den vereinbarten Speicherfristen
- Löschung oder Sperrung bei Vertragsende und kontrollierte Überschreibung von Backups

- Dokumentierte Behandlung gesetzlicher Aufbewahrungspflichten
- Sichere Löschung oder Wiederverwendung von Datenträgern und virtuellen Ressourcen

8 Unterauftragnehmer und Drittlandzugriffe

- Datenschutzrechtliche und sicherheitsbezogene Prüfung vor Beauftragung
- Vertragliche Weitergabe der Pflichten aus dieser Vereinbarung
- Dokumentation der Verarbeitungsorte und eingesetzten Transfermechanismen
- Kein dauerhafter administrativer Zugriff aus Drittländern; notwendige Zugriffe sind einzeln freizugeben, zeitlich zu begrenzen und zu protokollieren

Anlage 3 Genehmigte Unterauftragnehmer

Diese Liste ist vor dem produktiven Vertragseinsatz mit den tatsächlichen Vertragspartnern, Anschriften, Regionen und Transfergrundlagen zu vervollständigen.

Unterauftragnehmer	Leistung	Datenarten	Ort	Grundlage
[HOSTER / ANSCHRIFT]	Hosting, Datenbank und Backups	Kundendaten und Protokolle	[ORT]	[AVV / GRUNDLAGE]
[KI-DIENST / ANSCHRIFT]	KI-Inferenz zur Entwurfserstellung	Freigegebene E-Mail-Inhalte und Kontext	[REGION]	[AVV / ZERO-RETENTION / TRANSFER]
[SUPPORT / ANSCHRIFT]	Entwicklung und Support, soweit ein Produktivzugriff möglich ist	Potenzielle Sichtbarkeit von Kundendaten im Supportfall	[ZUGRIFFSORT]	[AVV / SCC / TIA / ZUSATZMASSNAHMEN]
[WEITERER DIENSTLEISTER]	[LEISTUNG]	[DATENARTEN]	[ORT]	[VERTRAGLICHE GRUNDLAGE]

Änderungen dieser Liste erfolgen nach dem Verfahren in Ziffer 6. Ein Dienstleister darf erst dann auf personenbezogene Daten zugreifen, wenn die erforderlichen Verträge und gegebenenfalls Drittlandgarantien wirksam abgeschlossen sind.