

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO zwischen den folgenden Vertragsparteien.

Verantwortlicher

Kunde

Der im Rahmen der Registrierung für <https://getdone.dev.luma-it.at> angegebene Kunde

Nachfolgend „Verantwortlicher“ oder „Kunde“

und

Auftragsverarbeiter

LUMA-IT GmbH

Laskahofstraße 14/4/46, 4030 Linz, Österreich

[E-Mail: office@getdone.at](mailto:office@getdone.at)

Nachfolgend „Auftragsverarbeiter“ oder „Anbieter“

Zuletzt aktualisiert: 15.08.2026

GetDone

Ein Produkt der LUMA-IT GmbH

Gegenstand und Geltungsbereich

Diese Vereinbarung gilt für die Verarbeitung personenbezogener Daten durch den Anbieter im Auftrag des Kunden im Zusammenhang mit der Nutzung der SaaS-Anwendung GetDone unter <https://getdone.dev.luma-it.at>.

Sie gilt ausschließlich für Verarbeitungen, bei denen der Kunde beziehungsweise die von ihm vertretene Organisation Verantwortlicher im Sinne des Art. 4 Z 7 DSGVO und der Anbieter Auftragsverarbeiter gemäß Art. 28 DSGVO ist.

Soweit der Anbieter personenbezogene Daten in eigener datenschutzrechtlicher Verantwortung verarbeitet, insbesondere zur Vertrags- und Benutzerverwaltung, Abrechnung, IT-Sicherheit, Missbrauchsprävention oder Erfüllung gesetzlicher Verpflichtungen, findet diese Vereinbarung

keine Anwendung.

Diese Vereinbarung wird mit Abschluss der Registrierung Bestandteil des Nutzungsvertrags und bedarf keiner gesonderten Unterzeichnung.

Gegenstand, Dauer, Art und Zweck der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung und der Betrieb von GetDone für den Kunden.

Die Verarbeitung erfolgt für die Dauer des Nutzungsvertrags und solange der Anbieter personenbezogene Daten im Auftrag des Kunden verarbeitet.

Die Verarbeitung umfasst insbesondere das Erfassen, Speichern, Organisieren, Ändern, Auslesen, Bereitstellen, Übermitteln innerhalb der vorgesehenen Berechtigungsstrukturen, Protokollieren, Sichern und Löschen personenbezogener Daten.

Zweck der Verarbeitung ist insbesondere die Bereitstellung der Aufgaben-, Benutzer-, Berechtigungs-, Organisations-, Kommentar-, Datei-, Benachrichtigungs-, Protokollierungs- und Auswertungsfunktionen von GetDone sowie der technische Betrieb, die Wartung, Datensicherung und Sicherheit der Anwendung.

Datenarten und betroffene Personen

Je nach Nutzung durch den Kunden können insbesondere folgende Daten verarbeitet werden:

- Stamm- und Kontaktdaten,
- Benutzer-, Organisations- und Berechtigungsdaten,
- Aufgaben- und Inhaltsdaten,
- Kommentare und Dateianhänge,
- Nutzungs-, Aktivitäts- und Protokolldaten,
- organisatorische Zuordnungen,
- sonstige personenbezogene Daten, die der Kunde oder seine Benutzer innerhalb der vorgesehenen Funktionen von GetDone eingeben.

Betroffene Personen können insbesondere sein:

- Mitarbeiter und sonstige Beschäftigte des Kunden,
- Benutzer und Administratoren,
- Kunden und Interessenten des Kunden,
- Geschäftspartner, Lieferanten und Dienstleister,
- sonstige Personen, deren Daten der Kunde über GetDone verarbeitet.

Der Kunde entscheidet darüber, welche personenbezogenen Daten und Kategorien betroffener Personen tatsächlich verarbeitet werden.

Weisungsgebundene Verarbeitung

Der Anbieter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, soweit keine gesetzliche Verpflichtung zu einer darüber hinausgehenden Verarbeitung besteht.

Die Weisungen ergeben sich insbesondere aus dem Nutzungsvertrag, dieser Vereinbarung sowie den vom Kunden und seinen berechtigten Benutzern innerhalb der Anwendung vorgenommenen Einstellungen und Handlungen.

Weitere Weisungen können in Textform erteilt werden.

Ist der Anbieter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt, informiert er den Kunden hierüber unverzüglich.

Vertraulichkeit und Sicherheit

Der Anbieter stellt sicher, dass zur Verarbeitung personenbezogener Daten befugte Personen zur Vertraulichkeit verpflichtet sind oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Anbieter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die wesentlichen Maßnahmen sind in **Anlage 1 – Technische und organisatorische Maßnahmen** beschrieben.

Der Anbieter darf die Maßnahmen entsprechend der technischen Weiterentwicklung anpassen, sofern das vereinbarte Schutzniveau hierdurch nicht unterschritten wird.

Unterstützung des Kunden

Der Anbieter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen angemessen bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen.

Dies umfasst insbesondere die Unterstützung

- bei der Bearbeitung von Betroffenenrechten gemäß Kapitel III DSGVO,
- bei der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO,
- bei Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DSGVO sowie
- soweit erforderlich bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen gemäß Art. 35 und 36 DSGVO.

Erhält der Anbieter ein Betroffenenbegehren zu Daten, für die der Kunde Verantwortlicher ist, wird dieses grundsätzlich an den Kunden weitergeleitet.

Datenschutzverletzungen

Der Anbieter informiert den Kunden unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die vom Anbieter im Auftrag des Kunden verarbeitete Daten betrifft.

Der Anbieter stellt dem Kunden die ihm verfügbaren Informationen zur Verfügung, die dieser zur Erfüllung seiner gesetzlichen Melde- und Informationspflichten benötigt.

Unterauftragsverarbeiter

Der Kunde erteilt dem Anbieter eine allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter gemäß Art. 28 Abs. 2 DSGVO.

Die derzeit eingesetzten Unterauftragsverarbeiter sind in **Anlage 2 – Unterauftragsverarbeiter** aufgeführt.

Der Anbieter informiert den Kunden rechtzeitig über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern. Der Kunde kann einer Änderung aus sachlich begründeten datenschutzrechtlichen Gründen widersprechen

Der Anbieter verpflichtet eingesetzte Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die den Anforderungen des Art. 28 DSGVO entsprechen.

Der Anbieter bleibt für die Erfüllung der datenschutzrechtlichen Pflichten seiner Unterauftragsverarbeiter nach Maßgabe der gesetzlichen Bestimmungen verantwortlich.

Drittlandübermittlungen

Personenbezogene Daten werden außerhalb des Europäischen Wirtschaftsraums nur verarbeitet oder übermittelt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Hierfür können insbesondere ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO oder geeignete Garantien gemäß Art. 46 DSGVO, insbesondere Standardvertragsklauseln der Europäischen Kommission, herangezogen werden.

Löschung und Rückgabe

Nach Beendigung der Auftragsverarbeitung löscht oder gibt der Anbieter die im Auftrag des Kunden verarbeiteten personenbezogenen Daten nach Wahl des Kunden zurück, soweit keine gesetzliche Verpflichtung zur weiteren Speicherung besteht.

Soweit keine Rückgabe verlangt wird, werden die Daten nach Maßgabe des vereinbarten Löschkonzepts gelöscht.

Gelöschte Daten können vorübergehend noch in Sicherungskopien enthalten sein. Backups werden turnusmäßig überschrieben beziehungsweise gelöscht und höchstens 30 Tage aufbewahrt. Aufgrund der Multi-Tenancy-Architektur ist eine isolierte Löschung einzelner Kundendaten aus

bestehenden Backups technisch nicht vorgesehen.

Nachweise und Kontrollen

Der Anbieter stellt dem Kunden die zur Nachweisung der Einhaltung von Art. 28 DSGVO erforderlichen Informationen zur Verfügung und ermöglicht angemessene Überprüfungen.

Soweit möglich, erfolgen Nachweise zunächst durch geeignete Dokumentationen, Sicherheitsinformationen, Prüfberichte oder vergleichbare Unterlagen.

Erforderliche weitergehende Prüfungen sind rechtzeitig anzukündigen und so durchzuführen, dass der Geschäftsbetrieb sowie die Sicherheit und Vertraulichkeit anderer Kunden nicht unangemessen beeinträchtigt werden.

Gesetzliche Kontrollrechte der Datenschutzaufsichtsbehörden bleiben unberührt.

Schlussbestimmungen

Soweit diese Vereinbarung keine abweichenden Regelungen enthält, gelten ergänzend der Nutzungsvertrag und die Allgemeinen Geschäftsbedingungen für GetDone.

Im Fall eines Widerspruchs zwischen dieser Vereinbarung und den Allgemeinen Geschäftsbedingungen gehen hinsichtlich der Auftragsverarbeitung die Bestimmungen dieser Vereinbarung vor.

Änderungen dieser Vereinbarung dürfen die gesetzlichen Anforderungen des Art. 28 DSGVO nicht unterschreiten.

Anlagen

Anlage 1 – Technische und organisatorische Maßnahmen

Der Anbieter setzt insbesondere folgende Maßnahmen ein:

- Hosting der primären Anwendung auf Servern in Österreich,
- logische Trennung der Kundenorganisationen innerhalb der Multi-Tenancy-Architektur,
- rollen- und berechtigungsbasierte Zugriffskontrolle,
- administrative Zugriffe nur für entsprechend berechtigte Personen,
- Verpflichtung zugriffsberechtigter Personen auf Vertraulichkeit,
- Speicherung von Passwörtern ausschließlich als kryptografische Hashwerte,
- TLS-/HTTPS-Verschlüsselung bei der Datenübertragung,
- Einsatz technischer Schutzmaßnahmen gegen unbefugte oder missbräuchliche Zugriffe,
- Protokollierung sicherheits- und anwendungsrelevanter Vorgänge,
- tägliche automatisierte Sicherungen von Datenbank und Dateianhängen,
- verschlüsselte Speicherung der Backups,
- Aufbewahrung der Backups für höchstens 30 Tage,
- Speicherung der Backups in der AWS-Region Frankfurt, Deutschland,

- Verfahren zur Vergabe und Entziehung von Zugriffsberechtigungen,
- Verfahren zur Behandlung von Sicherheitsvorfällen,
- regelmäßige Überprüfung und Weiterentwicklung der Sicherheitsmaßnahmen.

Anlage 2 – Unterauftragsverarbeiter

Zum Zeitpunkt des Abschlusses dieser Vereinbarung werden insbesondere folgende Unterauftragsverarbeiter eingesetzt:

netcup GmbH, Deutschland

Hosting und Server-Infrastruktur; eingesetzter Serverstandort für GetDone: Österreich.

Laravel Holdings Inc., USA – Laravel Forge

Technische Verwaltung und Administration der Server-Infrastruktur. Drittlandübermittlungen erfolgen, soweit erforderlich, nach Maßgabe der Art. 44 ff. DSGVO.

Cloudflare, Inc., USA

Reverse Proxy, CDN sowie Sicherheits- und Schutzfunktionen. Drittlandübermittlungen erfolgen, soweit anwendbar, auf Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien gemäß Art. 46 DSGVO.

Maileroo Group Pty Ltd., Australien

Versand transaktionaler und systembezogener E-Mails. Drittlandübermittlungen erfolgen, soweit erforderlich, auf Grundlage geeigneter Garantien gemäß Art. 46 DSGVO.

Amazon Web Services

Speicherung verschlüsselter Backups in der AWS-Region Frankfurt, Deutschland. Soweit eine Drittlandübermittlung erfolgt, gelten die Anforderungen der Art. 44 ff. DSGVO.