Frontify

# Auftragsverarbeitungs-vereinbarung

Frontify AG, Version: März 2026
Datum auswählen

| zwischen | und |
| --- | --- |
| **Firma**<br>Strasse<br>PLZ Ort<br>Land | **Frontify AG**<br>Unterstraße 4<br>9000 St. Gallen<br>Schweiz |
| im Folgenden als "Kunde" oder "Partei" bezeichnet | im Folgenden als "Frontify" oder "Partei" bezeichnet und zusammen mit dem Kunden als die "Parteien" bezeichnet |

# Inhaltsübersicht

Frontify

Frontify

# 1. Präambel

Im Rahmen der Erbringung der Frontify-Dienste gemäss dem Vertrag zwischen Frontify und dem Kunden kann Frontify personenbezogene Daten im Auftrag des Kunden verarbeiten. Die Parteien verpflichten sich, die Bedingungen dieser Auftragsverarbeitungsvereinbarung einschließlich ihrer Anhänge (zusammen als **"AVV"** bezeichnet) einzuhalten. Der AVV bildet mit Unterzeichnung des Vertrages automatisch einen integralen Bestandteil des Vertrages durch Verweis. Im Falle eines Widerspruchs zwischen den Bestimmungen der AVV und den Bestimmungen des Vertrages sind die Bestimmungen der AVV massgeblich.

Die Parteien erkennen an und vereinbaren, dass der Kunde als Verantwortlicher oder Auftragsverarbeiter in Bezug auf personenbezogene Daten seines Personals, seiner Dienstleister, Lieferanten und/oder anderer vom Kunden einbezogener Dritter (**"personenbezogene Daten des Kunden"**) gelten kann. Infolgedessen ist festzuhalten,

- dass Frontify ein Auftragsverarbeiter ist, wenn der Kunde als Verantwortlicher gilt,
- und dass Frontify ein Unterauftragsverarbeiter ist, wenn der Kunde als Auftragsverarbeiter gilt.

Diese AVV spiegelt die Verpflichtung der Parteien wider, die Datenschutzgesetze in Bezug auf die Verarbeitung personenbezogener Daten des Kunden im Rahmen des Vertrages einzuhalten. Die Kategorien der personenbezogenen Daten und der betroffenen Personen, die im Rahmen dieser AVV verarbeitet werden, sowie der Gegenstand, die Dauer und die Art der Verarbeitung sind in Anhang A (Gegenstand und Einzelheiten der Verarbeitungstätigkeiten) näher beschrieben.

# 2. Begriffsbestimmungen

Sofern in dieser AVV oder im Vertrag nicht anders definiert, haben alle in diesem Abschnitt aufgelisteten Begriffe die angegebene Bedeutung.

**„Angemessenes Drittland"** bezeichnet (i) im Falle der Anwendbarkeit der DSGVO ein Land, für das die Europäische Kommission einen Angemessenheitsbeschluss im Sinne von Art. 45(1) erlassen hat, (ii) im Falle der Anwendbarkeit des Datenschutzgesetzes des Vereinigten Königreichs ein Land, für das ein Angemessenheitsbeschluss gemäß Abschnitt 17A des Data Protection Act 2018 erlassen wurde, und (iii) im Falle der Anwendbarkeit des Schweizer Datenschutzgesetzes ein Land, das in Anhang 1 der Verordnung über den Datenschutz (SR 235.11) aufgeführt ist.

**”Antrag der betroffenen Person”** ist ein Gesuch, das von einer betroffenen Person gestellt wird, um das Recht der betroffenen Person auf Auskunft, Berichtigung, Löschung, Übertragung oder Portierung personenbezogener Daten des Kunden oder auf Einschränkung oder Widerspruch der Verarbeitung personenbezogener Daten des Kunden gemäss Kapitel III der DSGVO auszuüben.

**”Auftragsverarbeiter”** bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

**”Betroffene Person**” ist die natürliche Person, auf die sich die personenbezogenen Daten beziehen.

**”Datenschutzgesetz des Vereinigten Königreichs”** bezeichnet den Data Protection Act 2018 und die United Kingdom General Data Protection Regulation.

**”Datenschutzgesetze**” bezeichnet alle Gesetze und Vorschriften, die auf die Verarbeitung personenbezogener Daten im Rahmen des Vertrages anwendbar sind, einschließlich, aber nicht beschränkt auf die DSGVO, die Gesetze des EWR und seiner Mitgliedsstaaten, sowie die Gesetze der Schweiz, der Vereinigten Staaten von Amerika und des Vereinigten Königreichs.

**”Datum des Inkrafttretens**” bedeutet das Datum des Inkrafttretens des Vertrages.

”**DSGVO**” bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

**”EWR**” bezeichnet den Europäischen Wirtschaftsraum.

**”Frontify**” bezeichnet die Frontify AG.

**”Frontify-Dienste**” bezeichnet die von Frontify angebotenen und vom Kunden im Rahmen des Vertrages erworbenen Produkte und Dienstleistungen, sowohl aktuell als auch in Zukunft, einschließlich des Rechts und/oder der Lizenz zur Nutzung der Frontify-Plattform.

**”Frontify-Plattform”** bezeichnet die Software, die Frontify dem Kunden zur Nutzung über das Internet zur Verfügung stellt, namentlich die von Frontify angebotene webbasierte All-in-One Markenmanagement-SaaS-Lösung, die mobile App und die Desktop-App.

**“KI-Funktionen”** bezeichnet Funktionen auf Basis von künstlicher Intelligenz oder des

maschinellen Lernens, die Frontify innerhalb der Frontify-Plattform anbieten kann, um die Verwaltung von Assets zu optimieren und die Markenkonsistenz zu unterstützen.

**"Kunde"** umfasst, ausschliesslich für die Zwecke dieser AVV und sofern nicht anders vereinbart, den Kunden von Frontify im Rahmen des Vertrages, einschliesslich der verbundenen Unternehmen des Kunden.

**„Benachrichtigungs-E-Mail-Adresse des Kunden"** bezeichnet die E-Mail-Adresse, die im Vertrag als Kontaktadresse des Kunden für rechtliche und/oder datenschutzrechtliche Benachrichtigungen angegeben ist; oder, falls im Vertrag keine E-Mail-Adresse angegeben ist, die E-Mail-Adresse eines oder mehrerer Kundenkontakte in den Aufzeichnungen von Frontify.

**„Benachrichtigungs-E-Mail-Adresse von Frontify"** bezeichnet privacy@frontify.com.

**"Kundendaten**" sind alle Daten, einschließlich personenbezogener Daten des Kunden, die vom Kunden, seinen verbundenen Unternehmen oder seiner Plattform Nutzer über die Frontify-Dienste übermittelt, gespeichert, gesendet oder empfangen werden.

**"Laufzeit"** bezeichnet den Zeitraum ab dem Datum des Inkrafttretens bis zur Beendigung der Erbringung der Frontify-Dienste, gegebenenfalls einschliesslich eines Zeitraums, in dem die Erbringung der Frontify-Dienste ausgesetzt wurde, und eines Zeitraums nach der Beendigung, in dem die Frontify-Dienste zu Übergangszwecken weiter erbracht werden.

**"Plattform Nutzer**" bezeichnet jede natürliche Person, die berechtigt ist, die Frontify-Dienste gemäss dem Vertrag zu nutzen.

**"Personenbezogene Daten**" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare betroffene Person beziehen; als identifizierbar wird eine betroffene Person angesehen, die direkt oder indirekt identifiziert werden kann.

**"Produkte und Dienste von Drittanbietern"** sind unabhängige Produkte und Dienste von Drittanbietern, die nicht direkt durch Frontify lizenziert werden, einschliesslich, jedoch nicht beschränkt auf webbasierte, mobile, offline oder andere Softwarefunktionen, die mit den Frontify-Diensten interagieren. Produkte und Dienste von Drittanbietern können vom Kunden oder einem Drittanbieter bereitgestellt und nach Wahl des Kunden aktiviert werden, um die Erfahrung und Funktionalität der Frontify-Dienste zu erweitern.

**"Schweizer Datenschutzgesetz"** bedeutet das Bundesgesetz über den Datenschutz (SR 235.1) und die Verordnung über den Datenschutz (SR 235.11).

**”Standardvertragsklauseln” oder ”SCC”** bezeichnet den Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung Personenbezogener Daten in Drittländer gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

**”Technische und organisatorische Massnahmen”** oder **”TOMs”** bezeichnet eine Reihe von Regeln, Leitlinien, Richtlinien und Verfahren, die sicherstellen sollen, dass alle Nutzer, Server, Netzwerke und Prozesse innerhalb einer Organisation das angemessene Sicherheitsniveau und die Datenschutzstandards gemäss den Datenschutzgesetzen erfüllen.

”**Unterauftragsverarbeiter**” bezeichnet jeden Drittanbieter, der von Frontify beauftragt wird, personenbezogene Daten des Kunden im Rahmen der Erbringung der Frontify-Dienste zu verarbeiten.

**”Verantwortlicher**” bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt.

**”Verarbeitung**” oder ”**Verarbeitungstätigkeit**” bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

**”Verbundenes Unternehmen”** bedeutet jedes Unternehmen, das direkt oder indirekt das betreffende Unternehmen kontrolliert, von ihm kontrolliert wird oder unter gemeinsamer Kontrolle mit ihm steht. ”**Kontrolle**” im Sinne dieser Definition bedeutet das direkte oder indirekte Eigentum an oder die Macht über mehr als 50 % der stimmberechtigten Anteile des betreffenden Unternehmens oder die Möglichkeit, die Finanz- und Geschäftspolitik zu bestimmen oder die Geschäftsführung des betreffenden Unternehmens zu ernennen.

**”Vertrag”** bezeichnet den Frontify-Lizenzvertrag, das Bestellformular oder einen anderen schriftlichen oder elektronischen Vertrag, der zwischen Frontify und dem Kunden für die Nutzung der Frontify-Dienste geschlossen wurde, einschließlich aller Anhänge, insbesondere, aber nicht beschränkt auf das Angebot, die AGB, das Service Level Agreement und jedes andere zusätzliche Dokument, das das Vertragsverhältnis zwischen den Parteien regelt.

Frontify

# 3. Durchführung und Dauer

## 3.1. Einführung

Diese AVV ist integraler Bestandteil des Vertrages und muss nicht separat unterzeichnet werden. Jede Partei schließt diese AVV in ihrem eigenen Namen und, soweit nach den Datenschutzgesetzen erforderlich und/oder zulässig, im Namen und im Auftrag ihrer verbundenen Unternehmen ab.

Diese AVV wird ab dem Datum des Inkrafttretens rechtsverbindlich und ersetzt alle zuvor von den Parteien vereinbarten Bestimmungen zum Datenschutz, zur Datenverarbeitung und/oder zur Datensicherheit. Diese AVV endet automatisch mit der Beendigung des Vertrages oder mit einer früheren Beendigung gemäss den hierin festgelegten Bedingungen.

## 3.2. Bestandteile dieser AVV

Diese AVV besteht aus vier (4) Teilen:

- Der Hauptteil der AVV;
- Anhang A (Gegenstand und Einzelheiten der Verarbeitungstätigkeiten);
- Anhang B (Liste der Unterauftragsverarbeiter);
- Anhang C (Technische und organisatorische Massnahmen)

# 4. Rollen und Einhaltung von Vorschriften

## 4.1. Verantwortlicher und Auftragsverarbeiter

In Übereinstimmung mit ihren jeweiligen Rollen und unter Einhaltung der Datenschutzgesetze erkennen der Kunde in seiner Eigenschaft als Verantwortlicher oder Auftragsverarbeiter und Frontify in seiner Eigenschaft als Auftragsverarbeiter oder Unterauftragsverarbeiter an und vereinbaren, dass:

a) der Gegenstand und die Einzelheiten der Verarbeitungstätigkeit in Anhang A beschrieben sind;
b) jede Partei den Verpflichtungen aus den Datenschutzgesetzen in Bezug auf die Verarbeitung personenbezogener Daten des Kunden nachkommen wird.

### 4.2. Ermächtigung durch eine Drittpartei in der Funktion des Verantwortlichen

Soweit der Kunde ein Auftragsverarbeiter ist, gewährleistet der Kunde, dass die Anweisungen und Handlungen des Kunden in Bezug auf die personenbezogenen Daten des Kunden, einschliesslich der Ernennung von Frontify als Unterauftragsverarbeiter, von dem jeweiligen für die Verarbeitung Verantwortlichen ordnungsgemäss genehmigt worden sind.

## 5. Auftragsverarbeitung

### 5.1. Umfang der Verarbeitung

Mit dem Abschluss dieser AVV vereinbaren die Parteien, dass Frontify personenbezogene Daten des Kunden nur im Zusammenhang mit der Erbringung der Frontify-Dienste und/oder auf dokumentierte Anweisung des Kunden verarbeitet.

Der Gegenstand und die Einzelheiten der Verarbeitung sind in Anlage A aufgeführt, und Frontify wird sich ausschliesslich auf diese stützen, es sei denn, eine weitere Verarbeitung ist (a) durch anwendbare Gesetze vorgeschrieben, (b) basiert auf dokumentierten Anweisungen des Kunden oder (c) wurde von den Parteien anderweitig schriftlich vereinbart. Wenn und soweit anwendbare Gesetze eine weitere Verarbeitung der personenbezogenen Daten des Kunden erfordern, wird Frontify den Kunden, soweit gesetzlich zulässig, unverzüglich per E-Mail an die Benachrichtigungs-E-Mail-Adresse des Kunden informieren.

Frontify benachrichtigt den Kunden, wenn Frontify der Ansicht ist, dass die dokumentierten Anweisungen des Kunden gegen Datenschutzgesetze verstossen, und ist berechtigt, die Ausführung der betreffenden Anweisung auszusetzen, bis der Kunde eine datenschutzkonforme Anweisung erteilt. Wenn die dokumentierten Anweisungen des Kunden gegen Datenschutzgesetze verstossen, stellt der Kunde Frontify von allen Ansprüchen, Schäden und Verbindlichkeiten, die sich aus solchen Anweisungen ergeben, frei und hält Frontify schadlos.

### 5.2. Rechtmässigkeit der Verarbeitung

Der Kunde verpflichtet sich, bei der Nutzung der Frontify-Dienste und der Erteilung von Anweisungen die personenbezogenen Daten des Kunden in Übereinstimmung mit den Anforderungen der Datenschutzgesetze zu verwenden und zu verarbeiten, einschliesslich, aber nicht beschränkt auf die Verpflichtung, die betroffenen Personen über die Verwendung von Frontify als Auftragsverarbeiter zu informieren. Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmässigkeit der

personenbezogenen Daten des Kunden und dafür, wie der Kunde die personenbezogenen Daten des Kunden gesammelt hat.

## 5.3. Löschung oder Rückgabe von persönlichen Daten des Kunden

Während der Laufzeit ermöglicht Frontify dem Kunden und/oder den Plattform Nutzern, Kundendaten über die Funktionalitäten der Frontify-Dienste zu löschen. Wenn der Kunde oder ein Plattform Nutzer Kundendaten löscht, werden diese in Übereinstimmung mit dem anwendbaren Recht aus den Systemen von Frontify entfernt.

Nach Beendigung des Vertrags und auf schriftliche Anfrage stellt Frontify dem Kunden eine Kopie der Kundendaten auf einem handelsüblichen Datenträger oder durch elektronische Übertragung in einem von den Parteien vereinbarten Format zur Verfügung. Neunzig (90) Tage nach dem Datum des Inkrafttretens der Beendigung des Vertrages oder auf Verlangen des Kunden auch schon vorher wird Frontify alle Kundendaten löschen, es sei denn, dies ist aufgrund gesetzlicher Aufbewahrungspflichten nicht möglich.

Frontify kann Kundendaten aufbewahren, die (a) in einem archivierten Computersystem-Backup in Übereinstimmung mit Sicherheits- und/oder Disaster-Recovery-Verfahren enthalten sind; (b) in latenten Daten enthalten sind, einschließlich gelöschter Dateien und anderer nicht logischer Datentypen wie Speicherabzüge, Auslagerungsdateien, temporäre Dateien, Drucker-Spool-Dateien und Metadaten, die ohne den Einsatz spezieller Tools und Techniken nicht allgemein abrufbar oder zugänglich sind; (c) zu Zwecken der Einhaltung gesetzlicher Vorschriften, der Archivierung oder der Aufbewahrung von Aufzeichnungen in Übereinstimmung mit geltendem Recht erstellt werden; oder (d) zu Zwecken der Bestätigung der Einhaltung dieser AVV aufbewahrt werden, jeweils vorbehaltlich der Vernichtung dieser Kundendaten zu gegebener Zeit und der Unzugänglichkeit dieser Kundendaten durch Frontify und derer Angestellten im Rahmen des normalen Geschäftsbetriebs, und ferner, dass diese Kundendaten in jedem Fall den Bestimmungen der AVV unterliegen.

Personenbezogene Kundendaten, die im Computersystem-Backup gespeichert sind, werden automatisch nach dreihundertfünfundsechzig (365) Tagen ab der Erstellung des Backups gelöscht. Auf schriftliche Anfrage stellt Frontify dem Kunden eine Bestätigung aus, dass die personenbezogenen Kundendaten vollständig gelöscht worden sind.

Frontify

# 6. Unterauftragsverarbeitung

## 6.1. Beauftragung von Unterauftragsverarbeitern

Der Kunde ist generell damit einverstanden, dass Frontify Unterauftragsverarbeiter einsetzt, um seine vertraglichen Verpflichtungen aus dem Vertrag zu erfüllen. Daher genehmigt der Kunde die Beauftragung von verbundenen Unternehmen von Frontify und von Dritten als Unterauftragsverarbeiter, sofern die in diesem und Abschnitt 10 genannten Bedingungen eingehalten werden.

Frontify schliesst mit jedem Unterauftragsverarbeiter eine schriftliche Vereinbarung ab, die Datenschutzverpflichtungen enthält, die im Wesentlichen den in dieser DPA vereinbarten Verpflichtungen entsprechen, wobei Art, Umfang, Umstände und Zwecke der vom Unterauftragsverarbeiter erbrachten Dienstleistungen berücksichtigt werden.

Frontify stellt sicher, dass der Unterauftragsverarbeiter nur in dem Umfang auf Kundendaten zugreift und diese verarbeitet, wie es für die Erfüllung der an ihn übertragenen Verpflichtungen gemäss dem Vertrag, einschließlich dieser AVV, erforderlich ist.

Frontify haftet für alle an die Unterauftragsverarbeiter übertragenen Verpflichtungen sowie für alle Handlungen und Unterlassungen der Unterauftragsverarbeiter in demselben Umfang, in dem Frontify haften würde, wenn Frontify die Dienstleistungen jedes Unterauftragsverarbeiters gemäss den Bedingungen dieser AVV direkt erbringen würde. Sämtliche Haftungsbeschränkungen, die im Vertrag oder dieser AVV festgelegt sind, gelten auch für Handlungen und Unterlassungen der Unterauftragsverarbeiter.

## 6.2. Liste der Unterauftragsverarbeiter und Hinzuziehung neuer Unterauftragsverarbeiter

Die derzeitigen Unterauftragsverarbeiter von Frontify sind in Anhang B („**Liste der Unterauftragsverarbeiter**“) aufgeführt. Wenn ein neuer Unterauftragsverarbeiter beauftragt wird, aktualisiert Frontify die Liste der Unterauftragsverarbeiter und benachrichtigt den Kunden unter der Benachrichtigungs-E-Mail-Adresse des Kunden mindestens vierzehn (14) Tage bevor der neue Unterauftragsverarbeiter Zugriff auf die personenbezogenen Daten des Kunden erhält.

Der Kunde kann gegen jeden neuen Unterauftragsverarbeiter aus angemessenen und berechtigten Gründen Einspruch erheben (z. B. wenn die Einschaltung des neuen Unterauftragsverarbeiters gegen Datenschutzgesetze verstossen könnte). Falls der Kunde einem neuen Unterauftragsverarbeiter widerspricht, muss er dies innerhalb von vierzehn (14) Tagen seit der entsprechenden Benachrichtigung schriftlich an die Benachrichtigungs-E-Mail-Adresse von Frontify mitteilen und die spezifischen

Bedenken des Kunden bezüglich des neuen Unterauftragsverarbeiters darlegen, um Frontify die Möglichkeit zu geben, diese Bedenken zu berücksichtigen. Frontify wird sich in wirtschaftlich angemessener Weise bemühen, alle berechtigten Bedenken zu analysieren und kann nach eigenem Ermessen: (a) entscheiden, den neuen Unterauftragsverarbeiter nicht zu ernennen und/oder einen alternativen Unterauftragsverarbeiter vorzuschlagen; (b) Schritte unternehmen, um die spezifischen Bedenken des Kunden zu beheben oder zu entschärfen, und die schriftliche Zustimmung des Kunden zur Nutzung des neuen Unterauftragsverarbeiters einholen; oder (c) dem Kunden die Frontify-Dienste ohne die vom neuen Unterauftragsverarbeiter bereitgestellten Dienste oder Funktionen zur Verfügung stellen. Wenn Frontify nicht in der Lage ist oder nach vernünftigem Ermessen feststellt, dass es wirtschaftlich unzumutbar ist, eine der vorgenannten Möglichkeiten zu nutzen, kann der Kunde die betroffenen Teile der Frontify-Dienste durch schriftliche Mitteilung innerhalb von dreissig (30) Tagen ausserordentlich kündigen. Frontify erstattet dem Kunden anteilig alle im Voraus gezahlten Gebühren für die verbleibende Laufzeit nach dem wirksamen Kündigungsdatum in Bezug auf die gekündigten Frontify-Dienste, ohne dem Kunden eine Vertragsstrafe für diese Kündigung aufzuerlegen.

## 7. Rechte der betroffenen Person

Während der Laufzeit ermöglicht Frontify dem Kunden mit Hilfe der Funktionalitäten der Frontify-Dienste den Zugriff auf die personenbezogenen Daten des Kunden sowie deren Berichtigung, Einschränkung, Löschung und Export.

Falls ein Antrag einer betroffenen Person im Zusammenhang mit der Verarbeitung personenbezogener Daten des Kunden durch Frontify direkt an Frontify gerichtet wird, wird Frontify, sofern rechtlich zulässig, den Kunden entweder unverzüglich informieren und ihm die Einzelheiten des Antrags mitteilen, oder die betroffene Person auffordern, den Antrag direkt an den Kunden zu richten. Der Kunde ist für die Beantwortung eines Antrags der betroffenen Person verantwortlich, gegebenenfalls auch durch Nutzung der Funktionen der Frontify-Dienste.

Frontify unterstützt den Kunden bei der Erfüllung seiner Verpflichtungen nach den Datenschutzgesetzen, einschliesslich der Verpflichtung, auf Anträge von betroffenen Personen zu reagieren.

Frontify

# 8. Sicherheit

## 8.1. Technische und organisatorische Massnahmen (”TOMs”)

Frontify stellt die Einhaltung der durch die Datenschutzgesetze auferlegten Verpflichtungen in Bezug auf die Sicherheit der personenbezogenen Daten des Kunden sicher. Insbesondere wird Frontify unter Berücksichtigung Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung personenbezogener Daten des Kunden sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Massnahmen implementieren und aufrechterhalten, um ein dem Risiko angemessenes Schutzniveau im Sinne von Art. 32 DSGVO zu gewährleisten. Die TOMs sind integraler Bestandteil dieser AVV und sind als Anlage C beigefügt.

Die TOMs können sich im Laufe der Zeit ändern oder ersetzt werden. Frontify stellt jedoch sicher, dass eine solche Änderung oder ein solcher Ersatz niemals das angemessene Schutzniveau für die personenbezogenen Daten des Kunden beeinträchtigt.

## 8.2. Überprüfung und Berichte

Auf Anfrage des Kunden und unter der Voraussetzung, dass der Kunde zur Geheimhaltung verpflichtet ist, stellt Frontify dem Kunden (oder einem unabhängigen Drittprüfer des Kunden) Informationen über die Einhaltung der in dieser AVV dargelegten Verpflichtungen von Frontify zur Verfügung. Frontify beauftragt externe Prüfer mit der Überprüfung der Angemessenheit seiner Sicherheitsmassnahmen. Diese Überprüfungen werden (a) mindestens einmal jährlich auf der Grundlage der ISO 27001-Norm oder alternativer Normen, die der ISO 27001-Norm im Wesentlichen gleichwertig sind, durchgeführt; (b) von unabhängigen Sicherheitsexperten nach Wahl und auf Kosten von Frontify durchgeführt; und (c) führen zur Erstellung eines Prüfungsberichts (”Bericht”), welcher als vertrauliche Information von Frontify gilt. Auf schriftliche Anfrage des Kunden, stellt Frontify eine Kopie des Berichts zur Verfügung.

Wenn der Kunde trotz des Vorstehenden eine zusätzliche Überprüfung der Verfahren von Frontify in Bezug auf die personenbezogenen Daten des Kunden durchführen möchte, muss der Kunde Frontify einen entsprechenden Antrag stellen, und Frontify kann diesem Antrag zustimmen, sofern a) eine solche Überprüfung gemäss Datenschutzgesetz erforderlich ist; und b) eine ähnliche Überprüfung nicht bereits vor weniger als zwölf (12) Monaten durchgeführt wurde. Die vorstehenden Einschränkungen dürfen jedoch nicht die Durchführung einer solchen zusätzlichen Prüfung verhindern, wenn es Hinweise auf Datenschutzverstösse gibt und/oder die Überprüfung von einer Aufsichtsbehörde oder einer anderen zuständigen Regulierungsbehörde verlangt wird. Der Kunde erstattet Frontify die mit einer solchen

Frontify

Überprüfung verbundenen Kosten zu den jeweils gültigen Sätzen von Frontify, die dem Kunden auf Anfrage zur Verfügung gestellt werden. Vor Beginn einer solchen Überprüfung vereinbaren die Parteien einvernehmlich den Umfang, den Zeitpunkt und die Dauer sowie die Höhe der vom Kunden zu tragende Kostenerstattung. Alle Erstattungssätze müssen unter Berücksichtigung der von Frontify aufgewendeten Ressourcen angemessen sein. Der Kunde informiert Frontify unverzüglich über alle während einer Überprüfung festgestellten Verstösse, und Frontify unternimmt wirtschaftlich angemessene Anstrengungen, um alle von Frontify akzeptierten Verstösse zu beheben. Die Parteien verpflichten sich die Informationen im Zusammenhang mit einer solchen Überprüfung streng vertraulich zu behandeln.

## 8.3. Vertraulichkeit und Schulungen

Frontify stellt sicher, dass alle Mitarbeitenden und Dienstleistenden, die zur Verarbeitung von Kundendaten berechtigt sind, zur Geheimhaltung verpflichtet sind. Des Weiteren führt Frontify regelmäßig Schulungen für Mitarbeitende zu den Themen Datenschutz, Vertraulichkeit und Datensicherheit durch.

## 8.4. Management von Sicherheitsvorfällen und Benachrichtigung

Frontify unterhält Richtlinien und Verfahren für das Management von Sicherheitsvorfällen. Frontify benachrichtigt den Kunden unverzüglich, in jedem Fall aber innerhalb von 48 Stunden nach Bekanntwerden, über jede Verletzung in Bezug auf die personenbezogenen Daten des Kunden, die eine Benachrichtigung einer Aufsichtsbehörde, einer betroffenen Person oder des Kunden gemäss Datenschutzgesetz erforderlich machen könnte (**”Sicherheitsvorfall”**). Die Benachrichtigung über einen Sicherheitsvorfall erfolgt per E-Mail an die Benachrichtigungs-E-Mail-Adresse des Kunden und enthält mindestens die folgenden Angaben:

- eine Beschreibung der Art Sicherheitsvorfalls, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen des Sicherheitsvorfalls;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Massnahmen zur Behebung Sicherheitsvorfalls und gegebenenfalls Massnahmen zur Abmilderung dessen möglichen nachteiligen Auswirkungen.

Sollte es nicht möglich sein, die oben genannten Informationen gleichzeitig mit der Benachrichtigung zu übermitteln, so werden diese schnellstmöglich zu einem späteren Zeitpunkt nachgereicht.

Die Parteien vereinbaren, dass die Benachrichtigung von Frontify über einen Sicherheitsvorfall, nicht als Anerkennung eines Verschuldens oder einer Haftung von Frontify in Bezug auf den Sicherheitsvorfall angesehen wird. Frontify wird in wirtschaftlich vertretbarem Umfang mit dem Kunden zusammenarbeiten, um die Ursache eines solchen Sicherheitsvorfalls zu ermitteln, und, sofern die Behebung im Einflussbereich von Frontify liegt, angemessene Schritte zur Behebung dieser Ursache unternehmen. Sofern nicht durch Datenschutzgesetze vorgeschrieben, gelten die hierin enthaltenen Verpflichtungen nicht für Vorfälle, die durch den Kunden, Plattform Nutzer oder Produkte und Dienste von Drittanbietern verursacht werden.

## 9. KI-Funktionen und Datenverarbeitung

Im Zusammenhang mit der Bereitstellung der KI-Funktionen über die Frontify-Plattform ergreift Frontify alle erforderlichen technischen und organisatorischen Massnahmen, um eine verantwortungsvolle, sichere und konforme Verarbeitung gemäss den Datenschutzgesetzen und dieser AVV zu gewährleisten.

Frontify versichert, dass die KI-Funktionen zum Datum des Inkrafttretens ohne jegliche Verarbeitung funktionieren. Die Parteien erkennen jedoch an, dass eine zufällige Verarbeitung auftreten kann, wenn der Kunde personenbezogene Daten in Eingabeaufforderungen, Anweisungen oder Richtlinien an die KI-Funktionen einfügt, wenn personenbezogene Daten in den von der KI-Funktion generierten Ausgaben enthalten sind oder wenn personenbezogene Daten Teil anderer Kundendaten sind, die auf die Plattform hochgeladen oder anderweitig über die Plattform verfügbar gemacht werden (zusammenfassend „Inhaltsdaten“).

Soweit personenbezogene Daten im Zusammenhang mit den KI-Funktionen verarbeitet werden, wird Frontify: i) diese personenbezogenen Daten ausschliesslich zum Zweck der Bereitstellung von KI-Funktionen für den Kunden gemäß der Vereinbarung und den dokumentierten Anweisungen des Kunden verarbeiten; ii) personenbezogene Daten nicht für andere Zwecke verarbeiten, einschliesslich für das Training, die Entwicklung, die Verbesserung oder die Feinabstimmung von Modellen für künstliche Intelligenz oder maschinelles Lernen, es sei denn, diese Verarbeitung erfolgt ausschliesslich zum Nutzen des Kunden und führt nicht dazu, dass die personenbezogenen Daten zur Verbesserung von Modellen für andere Kunden oder zur allgemeinen Verwendung verwendet werden; oder es sei denn, der Kunde hat dies ausdrücklich schriftlich genehmigt.
Um die KI-Funktionen bereitzustellen, kann Frontify Drittanbieter von Technologien als Unterauftragsverarbeiter beauftragen. In diesem Fall stellt Frontify sicher, dass: i) diese Anbieter vor ihrer Beauftragung einer dokumentierten Datenschutz- und

Sicherheitsprüfung unterzogen werden; ii) mit jedem Unterauftragsverarbeiter eine schriftliche Datenverarbeitungsvereinbarung geschlossen wird, die im Wesentlichen die gleichen Verpflichtungen wie diese AVV enthält; iii) Unterauftragsverarbeitern vertraglich untersagt ist, Kundendaten für eigene Zwecke zu verwenden, einschliesslich für Modelltraining, -entwicklung oder -verbesserung; und iv) angemessene Verpflichtungen in Bezug auf Sicherheit, Vertraulichkeit und Reaktion auf Vorfälle vertraglich auferlegt werden.

Die Drittanbieter von KI-Lösungen, die derzeit von Frontify im Zusammenhang mit den KI-Funktionen beauftragt werden, sind in Anhang B aufgeführt. Alle diese Anbieter werden im Rahmen dieser AVV als Unterauftragsverarbeiter behandelt.
Frontify kann von Zeit zu Zeit neue KI-Funktionen einführen. Wenn eine solche Einführung zu wesentlichen Änderungen bei der Verarbeitung personenbezogener Daten oder zur Beauftragung neuer Unterauftragsverarbeiter führt, aktualisiert Frontify diese AVV und/oder die geltende Liste der Unterauftragsverarbeiter gemäss den hierin enthaltenen Bestimmungen für alle Unterauftragsverarbeiter.

## 10. Haftungsbegrenzung

Die Gesamthaftung jeder Partei und ihrer verbundenen Unternehmen, die sich aus dieser AVV ergibt oder mit ihr in Zusammenhang steht, unterliegt den im Vertrag vereinbarten Haftungsbeschränkungen.

## 11. Speicherstandort und Datenübertragungen

### 11.1. Speicherstandort

Entsprechend der vom Kunden im Vertrag getroffenen Festlegung werden die personenbezogenen Daten des Kunden auf Datenservern gespeichert, die sich im EWR oder in den USA befinden. Darüber hinaus werden die personenbezogenen Daten des Kunden am Hauptsitz von Frontify in der Schweiz verarbeitet. Eine Übermittlung von personenbezogenen Daten des Kunden an einen Ort ausserhalb eines angemessenen Drittlandes erfolgt nur, sofern die Datenschutzgesetze eingehalten werden und die in diesem Abschnitt 10 genannten Bedingungen erfüllt sind.

### 11.2. Datenübertragung nach der DSGVO

Sofern spezifische Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten des Kunden an einen Ort ausserhalb eines angemessenen Drittlandes erfordern,

vereinbaren die Parteien hiermit, dass Frontify die Einhaltung der Bestimmungen von Kapitel V der DSGVO durch die Implementierung der in Art. 46(2) DSGVO geforderten Massnahmen gewährleistet. Solche Massnahmen können unter anderem die Übermittlung personenbezogener Daten des Kunden (a) an einen Unterauftragsverarbeiter, dem verbindliche interne Datenschutzvorschriften gemäss Art. 47 DSGVO genehmigt wurden, oder (b) an einen Unterauftragsverarbeiter, der die Standardvertragsklauseln unterzeichnet hat, umfassen. Der jeweilige Datenübertragungsmechanismus für die einzelnen Unterauftragsverarbeiter ist in der Liste der Unterauftragsverarbeiter (Anhang B) aufgeführt.

Sollte ein Beschluss der Europäischen Kommission, der die Übermittlung personenbezogener Daten ausserhalb des EWR genehmigt, für ungültig erklärt werden oder eine Aufsichtsbehörde die Aussetzung der Übermittlung personenbezogener Daten verlangt, wird Frontify einen alternativen Datenübertragungsmechanismus implementieren, der es dem Kunden ermöglicht, die Frontify-Dienste unter Einhaltung der Datenschutzgesetze weiterhin zu nutzen.

### 11.3. Datenübertragung nach dem Datenschutzgesetz des Vereinigten Königreichs

Soweit das Datenschutzgesetz des Vereinigten Königreichs auf personenbezogene Daten des Kunden anwendbar ist und soweit es das Datenschutzgesetz des Vereinigten Königreichs erfordert, wird Frontify personenbezogene Daten des Kunden nur dann an einen Ort ausserhalb eines angemessenen Drittlandes übermitteln, sofern die anwendbaren Massnahmen gemäss dem Datenschutzgesetz des Vereinigten Königreichs und die Anweisungen des Information Commissioner des Vereinigten Königreichs umgesetzt wurden.

### 11.4. Datenübertragung nach dem Schweizer Datenschutzgesetz

Soweit das Schweizer Datenschutzgesetz auf personenbezogene Daten des Kunden anwendbar ist und soweit es das Schweizer Datenschutzgesetz erfordert, wird Frontify personenbezogene Daten des Kunden nur dann an einen Ort ausserhalb eines angemessenen Drittlandes übermitteln, sofern die anwendbaren Massnahmen gemäss dem Schweizer Datenschutzgesetz und die Anweisungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) umgesetzt wurden.

## 12. Kundenunterstützung und behördliche Anfragen

Auf Anfrage und soweit dies nach den Datenschutzgesetzen erforderlich ist, wird Frontify unter Berücksichtigung der Frontify zur Verfügung stehenden Informationen

und unter der Voraussetzung, dass der Kunde keinen anderen Zugang zu diesen Informationen hat, den Kunden in angemessener Weise bei der Erfüllung der einschlägigen Verpflichtungen gemäß Art. 32 bis 36 DSGVO unterstützen.

Falls Frontify gehalten ist, personenbezogene Daten des Kunden an Strafverfolgungs- oder andere staatliche Behörden herauszugeben, wird Frontify den Kunden, soweit gesetzlich zulässig, in geeigneter Weise benachrichtigen, damit der Kunde die Möglichkeit hat, geeignete Rechtsmittel gegen solche Herausgabeanordnungen zu ergreifen.

Soweit gesetzlich zulässig, erstattet der Kunde Frontify die mit einer solchen Kundenunterstützung verbundenen Kosten zu den jeweils gültigen Sätzen von Frontify, die dem Kunden auf Anfrage zur Verfügung gestellt werden.

# 13. Schlussbestimmungen

## 13.1. Salvatorische Klausel

Sollten einzelne Bestimmungen dieser AVV unwirksam oder unvollständig sein oder sollte die Erfüllung unmöglich sein, so berührt dies die Wirksamkeit der übrigen Bestimmungen dieser AVV nicht. Ungültige Bestimmungen sind durch eine gültige und zulässige Bestimmung zu ersetzen, die dem Inhalt der ursprünglichen Bestimmung in ihrem Sinngehalt am nächsten kommt.

## 13.2. Änderungen dieser AVV

Frontify kann diese AVV von Zeit zu Zeit ändern und wird wesentliche Änderungen im Voraus schriftlich ankündigen.
Der Kunde kann einer wesentlichen Änderung aus berechtigten Gründen widersprechen, indem er innerhalb von fünfzehn (15) Tagen nach Erhalt einer solchen Mitteilung schriftlich Widerspruch einlegt. Die Parteien werden den Widerspruch in gutem Glauben erörtern. Wenn die Parteien einen berechtigten Widerspruch nicht innerhalb einer angemessenen Frist beilegen können, bleibt die vorherige Fassung der AVV in Kraft, wobei jedoch alle Änderungen, die aufgrund geltender Datenschutzgesetze erforderlich sind, gemäss diesen Gesetzen in Kraft treten. Wenn der Kunde innerhalb der oben genannten Frist keinen Widerspruch einlegt, gilt die aktualisierte Fassung der AVV als akzeptiert.

## 13.3. Anwendbares Recht und Gerichtsstand

Diese AVV und alle Streitigkeiten oder Ansprüche, die sich aus oder im Zusammenhang mit ihr ergeben (einschliesslich ausservertraglicher Streitigkeiten oder Ansprüche),

unterliegen den im Vertragfestgelegten Bestimmungen zum anwendbaren Recht und zur Streitbeilegung und sind entsprechend auszulegen.

Wenn im Vertrag das anwendbare Recht oder der Gerichtsstand nicht festgelegt ist, unterliegt diese AVV dem Recht der Schweiz unter Ausschluss der Grundsätze des Kollisionsrechts und der ausschliesslichen Zuständigkeit der Gerichte in St. Gallen, Schweiz.

Frontify

# 14. Unterschriften

## Kunde

| Ort, Datum | Name, Titel | Unterschrift |
|---|---|---|
| Ort, Datum | Name, Titel | Unterschrift |

## Frontify AG

| Ort, Datum | Name, Titel | Unterschrift |
|---|---|---|
| Ort, Datum | Name, Titel | Unterschrift |

**Liste der Anhänge**

Anhang A: Gegenstand und Einzelheiten der Verarbeitung
Anhang B: Liste der Unterauftragsverarbeiter
Anhang C: Technische und organisatorische Massnahmen (TOMs)

Frontify

# Anhang A - Gegenstand und Einzelheiten der Verarbeitung

**Vertragsgegenstand.** Gegenstand ist die Bereitstellung der Frontify-Dienste und den dazugehörigen Support für den Kunden.

**Dauer der Verarbeitung.** Die Verarbeitungstätigkeiten werden während der Laufzeit durchgeführt, zuzüglich des Zeitraums nach Ablauf der Laufzeit bis zur Löschung aller personenbezogenen Daten des Kunden durch Frontify gemäss dieser AVV.

**Art und Zweck der Verarbeitung.** Frontify verarbeitet personenbezogene Daten des Kunden, die vom Kunden oder seinen Plattform Nutzern über die Frontify-Dienste übermittelt, gespeichert, gesendet oder empfangen werden, um die Frontify-Dienste und den dazugehörigen Support für den Kunden in Übereinstimmung mit dieser AVV bereitzustellen.

**Kategorien von personenbezogenen Daten.** Frontify verarbeitet im Zusammenhang mit den Frontify-Diensten die folgenden Kategorien personenbezogener Daten:

1. Für die Anmeldung erforderliche Pflichtangaben des Plattform Nutzers:
    - Name
    - E-Mail-Adresse

2. Auf freiwilliger Basis können die Plattform Nutzer die folgenden Informationen angeben:
    - Profilbild
    - Berufsbezeichnung
    - Unternehmen
3. Informationen zur Nutzung der Frontify-Plattform durch den Plattform Nutzer („Plattformnutzungsdaten”):

    - IP-Adresse
    - aus der IP-Adresse abgeleiteter geografischer Standort (auf regionaler Ebene)
    - Browsertyp und -version
    - Verweisquelle
    - Sprachpräferenz
    - Dauer der Besuche
    - Interaktionen mit Funktionen der Frontify-Plattform (z. B. aufgerufene Seiten, Download- und Upload-Verlauf)

    Diese Informationen können zu folgenden Zwecken erfasst werden: i) Betrieb, Wartung und Sicherheit der Frontify-Plattform, ii) Verbesserung der Qualität, des Designs und der Leistung der Frontify-Plattform, iii) Benachrichtigung der Plattform Nutzer über neue Funktionen, Dienste, Schulungen, Hilfeartikel, massgeschneiderte Berichte, Webinare und andere Veranstaltungen und iv) Einladung der Plattform Nutzer zur Teilnahme an Produktforschungsumfragen, zur Verbesserung ihrer Nutzererfahrung auf der Plattform..

Frontify

Frontify verarbeitet Plattformnutzungsdaten in der Regel in pseudonymisierter oder aggregierter Form. In bestimmten Fällen wird Frontify einen einzelnen Plattform Nutzer für einen der oben genannten Zwecke depseudonymisieren, wobei nur ausgewählte Mitarbeiter von Frontify Zugriff auf die depseudonymisierten Plattformnutzungsdaten haben, wenn dies zur Erfüllung einer erforderlichen Aufgabe notwendig ist.

4. Im Zusammenhang mit den Customer Hub-Diensten verarbeitete Informationen (einschliesslich der oben aufgeführten obligatorischen Plattformnutzerinformationen sowie der folgenden zusätzlichen Kategorien):

    - Terminplanungs- und Kalenderinformationen
    - Firmenname
    - Frontify-Benutzerrolle
    - Eindeutige Benutzer-IDs
    - Rechtlicher Ansprechpartner
    - Rechnungskontakt

5. In Assets eingebettete und/oder im Zusammenhang mit der Nutzung von KI-Funktionen verarbeitete Informationen:

    - Inhaltsdaten

    Das Hochladen von Inhaltsdaten wird ausschliesslich vom Kunden und den Plattform Nutzern verwaltet und unterliegt nicht der direkten Kontrolle von Frontify. Der Kunde und die Plattform Nutzer sind für die Nutzung der Inhaltsdaten und die Rechtmässigkeit der Verarbeitung verantwortlich und haftbar.

**Kategorien von betroffenen Personen.** Der Kunde legt selbständig fest, welche Personen Zugang zur Frontify-Platform erhalten sollen. In der Regel können die Plattform Nutzer in die folgenden Kategorien von betroffenen Personen eingeteilt werden:

- Arbeitnehmende des Kunden
- Auftragnehmende des Kunden (bspw. externe Berater/innen)

Frontify

# Anhang B - Liste der Unterauftragsverarbeiter

## Drittanbieter

| Anbieter | Firma des Anbieters | Adresse | Beschreibung der Dienstleistung | Datenhaltungs-frist | Ort der Daten-verarbeitung | Kategorien von personenbezogenen Daten | Kategorien von betroffenen Personen | Besondere Kategorien personenbezogener Daten | Mechanismus zur Datenübermittlung |
|---|---|---|---|---|---|---|---|---|---|
| **ActiveCampaign (Postmark)** | AC PM, LLC | 1 N Dearborn Street, Suite 500, Chicago, IL 60602, USA | Transaktions-E-Mail-Dienst | 45 Tage | USA | E-Mail-Adresse / IP-Adresse / geografischer Standort, der aus der IP-Adresse abgeleitet wird (regionale Ebene) / Öffnungsstatus | Plattform Nutzer | Nein | Angemessenheits-beschluss (Anbieter ist gemäss dem Data Privacy Framework zertifiziert) |
| **Amazon Web Services** | Amazon Web Services EMEA SARL | 38 Avenue John F. Kennedy, L-1855, Luxembourg, Luxembourg | Cloud-Dienstanbieter und KI-Dienste, inkl. Amazon Bedrock, Amazon Textract, und Amazon Rekognition, zur Unterstützung derKI-Features | Die Daten werden für die Dauer des Kundenvertrags gespeichert | Deutschland oder USA (gemäss individueller Vereinbarung zwischen Frontify und dem Kunden) | Alle Daten, die zur Ausführung der Frontify Plattform notwendig sind, inkl. aller Datenbankdaten. Inhaltsdaten für KI-Dienste | Plattform Nutzer | Nein | Angemessenheits-beschluss (Anbieter ist gemäss dem Data Privacy Framework zertifiziert) |
| **Amplitude** | Amplitude Inc. | 201 3rd Street, Suite 200, San Francisco, CA 94103, USA | Anonymisierte Produktanalytik | Die Daten werden innerhalb einer logischen Sekunde nach der Datenerfassung anonymisiert. | Deutschland | IP-Adresse / Plattformnutzungs-daten (anonymisiert) | Plattform Nutzer | Nein | Angemessenheits-beschluss (Anbieter ist gemäss dem Data Privacy Framework zertifiziert) |
| **Intercom** | Intercom R&D Unlimited Company | 2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Ireland | In-App-Support / Benutzereinführung / Feedbacksammlung / Produktneuigkeiten / Wissensdatenbank | Die Daten werden für die Dauer des Kundenvertrags gespeichert | USA | Name / E-Mail-Adresse / Plattformnutzungs-daten | Plattform Nutzer | Nein | Angemessenheits-beschluss (Anbieter ist gemäss dem Data Privacy Framework zertifiziert) |
| **Datadog** | Datadog Inc. | 620 8th Avenue, 45th Floor, New York, NY 10018-1741, USA | Kontrolle und Überwachung der Frontify-Plattform | 30 Tage | Deutschland | E-Mail-Adresse / IP-Adresse / Plattformnutzungs-daten | Plattform Nutzer | Nein | Angemessenheits-beschluss (Anbieter ist gemäss dem Data Privacy Framework zertifiziert) |
| **Splunk** | Splunk LLC | 250 Brannan Street, San Francisco, CA 94107, USA | Sicherheits-informationen und Ereignis-Management (SIEM) | 365 Tage | Deutschland | E-Mail-Adresse / IP-Adresse / Plattformnutzungs-daten | Plattform Nutzer | Nein | Angemessenheits-beschluss (Anbieter ist gemäss dem Data Privacy Framework zertifiziert) |
| **EverAfter** | EverAfter AI Ltd | 82 Yigal Alon, Tel Aviv, Israel 6789124 | Customer-Hub-Betrieb (einschließlich Onboarding und Aktivierung/Kommunikation und Updates/Self-Service-Support und Schulungen/Kontoverwaltung/automatisch | Die Daten werden für die Dauer des Kundenvertrags gespeichert | Deutschland | Name / E-Mail-Adresse / Terminplanung und Kalenderinformationen / Firmenname / Frontify-Benutzerrolle / Eindeutige Benutzer-ID) / Rechtlicher Ansprechpartner / Rechnungskontakt | Plattform Nutzer | Nein | Angemessenheits-beschluss |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | e Verlängerungen für Wachstum und und Self-Guided Kunden) | | | | | | |
| **Microsoft** | Microsoft Ireland Operations Limited | One Microsoft Place, South Country Business Park, Leopardstown Dublin 18, D18P521, Ireland | Azure-KI-Dienste zur Unterstützung der KI-Funktionen | 30 Tage | Deutschland | Inhaltsdaten | Plattform Nutzer | Nein | Angemessenheitsbeschluss<br><br>(Anbieter ist gemäss dem Data Privacy Framework zertifiziert) |
| **Langfuse** | Finto Technologies GmbH | Gethsemanestr. 4, 10437, Berlin, Deutschland | Überwachung und Analyse der Ein- und Ausgaben der KI-Funktionen | 90 Tage | Irland | Inhaltsdaten | Plattform Nutzer | Nein | Angemessenheitsbeschluss |

Frontify

## Tochtergesellschaften

| Anbieter | Firma des Anbieters | Adresse | Beschreibung der Dienstleistung | Datenhaltungs-frist | Ort der Daten-verarbeitung | Kategorien von personenbezogenen Daten | Kategorien von betroffenen Personen | Besondere Kategorien personenbezogener Daten | Mechanismus zur Datenübermittlung |
|---|---|---|---|---|---|---|---|---|---|
| **Frontify Inc.** | Frontify Inc. | 625 Broadway, Stockwerk 12, New York, NY 10012 | Supportdienste | Die Daten werden für die Dauer des Kundenvertrags gespeichert | USA / Deutschland | Name / E-Mail-Adresse / Plattformnutzungs-daten | Plattform Nutzer | Nein | SCC |
| **Frontify UK Ltd.** | Frontify UK Ltd. | 5 New Street Square, EC4A 3TW London | Supportdienste | Die Daten werden für die Dauer des Kundenvertrags gespeichert | England / Deutschland | Name / E-Mail-Adresse / Plattformnutzungs-daten | Plattform Nutzer | Nein | Angemessenheits-beschluss |
| **Frontify Deutschland GmbH** | Frontify Deutschland GmbH | Friedrich-Ebert-Anlage 36, 60325 Frankfurt am Main | Supportdienste | Die Daten werden für die Dauer des Kundenvertrags gespeichert | Deutschland | Name / E-Mail-Adresse / Plattformnutzungs-daten | Plattform Nutzer | Nein | Angemessenheits-beschluss |
| **TwicPics SAS** | TwicPics SAS | 10, rue de Penthievre, 75008 Paris, France | Supportdienste | Die Daten werden für die Dauer des Kundenvertrags gespeichert | Frankreich / Deutschland | Name / E-Mail-Adresse / Plattformnutzungs-daten | Plattform Nutzer | Nein | Angemessenheits-beschluss |

Frontify

# Anhang C - Technische und organisatorische Massnahmen (TOMs)

Frontify AG, Stand: April 2023

## 1. Präambel

Das Informationssicherheitsprogramm von Frontify wurde in Übereinstimmung mit Best-Practice-Branchenstandards wie ISO 27001 entwickelt. Die Sicherheitskontrollen von Frontify sind auf die Gegebenheiten eines Cloud-basierten Software-as-a-Service (SaaS)-Anbieters ausgerichtet. Die folgenden Ausführungen beziehen sich auf die Software von Frontify und die Erbringung der dazugehörigen Dienste (im Folgenden "Frontify-Dienste") und sind in diesem Zusammenhang wichtig für das Verständnis der Sicherheitsmassnahmen von Frontify.

Frontify hat geeignete technische und organisatorische Massnahmen (im Folgenden "TOMs") ergriffen, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko der Verarbeitungstätigkeiten, die zur Bereitstellung der Frontify-Dienste durchgeführt werden, angemessen ist. Die TOMs berücksichtigen den Stand der Technik, die Implementierungskosten und die Art, den Umfangs, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risikos für die Rechte und Freiheiten natürlicher Personen.

Die TOMs unterliegen regelmässigen Verbesserungen und Weiterentwicklungen; daher kann Frontify dieses Dokument von Zeit zu Zeit überprüfen und aktualisieren. In dieser Hinsicht ist Frontify berechtigt, angemessene alternative Massnahmen zu ergreifen, die das Gesamtsicherheitsniveau der hierin beschriebenen Massnahmen nicht wesentlich verringern dürfen.

Da Frontify die Dienste eines externen Hosting-Partners sowohl für das Hosting als auch für die Verarbeitung von Daten in Anspruch nimmt, werden einzelne Massnahmen ausschliesslich im Rechenzentrum dieses Hosting-Partners durchgeführt. Dementsprechend werden die TOMs, die nur den Hosting-Partner betreffen, in diesem Dokument mit dem Zusatz ("Hosting-Partner") gekennzeichnet.

Frontify

## 2. Überprüfungen und Zertifizierungen

Frontify stellt sicher, dass eine jährliche Überprüfung des implementierten Informationssicherheitsprogramms durch einen externen Prüfer durchgeführt wird, und stellt seinen Kunden auf Anfrage Nachweise der Einhaltung der Standards zur Verfügung, indem es Zertifikate (z. B. ISO 27001-Zertifizierung, Cyber Essentials-Zertifizierung) und Auszüge der Ergebnisse von Überprüfungen zur Verfügung stellt, unter der Bedingung, dass der Kunde zur Geheimhaltung verpflichtet ist.

## 3. Sicheres Cloud-Hosting

Die Frontify Dienste werden über die sichere Serverinfrastruktur unseres Cloud Hosting Partners AWS erbracht.

Weitere Informationen über die von AWS implementierten Sicherheitsstandards und finden Sie unter:

- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/programs/
- https://aws.amazon.com/compliance/data-center/controls/

## 4. Informationssicherheitsrichtlinie

Frontify hat eine Informationssicherheitsrichtlinie implementiert, welche alle relevanten Aspekte seines Sicherheitsprogramms regelt und mit Best-Practice-Branchenstandards wie den Anforderungen der ISO 27001 übereinstimmt. Die Informationssicherheitsrichtlinien von Frontify kann dem Kunden auf Anfrage zur Verfügung gestellt werden, unter der Bedingung, dass der Kunde zur Geheimhaltung verpflichtet ist. Weitere Informationen über die Sicherheitsmassnahmen von Frontify können unter https://www.frontify.com/en/security/ abgerufen werden.

## 5. Anonymisierung und Pseudonymisierung

Bei der Anonymisierung personenbezogener Daten werden persönliche Identifikatoren entfernt, Daten aggregiert oder so verarbeitet, dass sie nicht mehr mit einer einzelnen Person in Verbindung gebracht werden können. Bei der Pseudonymisierung wird der direkte Bezug zu einer einzelnen Person bei der Verarbeitung derart reduziert, dass erst durch die Aufnahme von Zusatzinformationen eine Zuordnung zu dieser Person möglich ist.

Soweit es technisch möglich und mit der Erbringung der Frontify Dienste vereinbar ist, anonymisiert Frontify die personenbezogenen Daten. Wenn eine Anonymisierung nicht möglich ist, greift Frontify auf die Pseudonymisierung von personenbezogenen Daten zurück. Um die Frontify-Dienste zu erbringen, ist eine Anonymisierung oder Pseudonymisierung personenbezogener Daten jedoch nicht in jedem Fall möglich und würde dem Zweck der Frontify-Dienste zuwiderlaufen.

# 6. Verschlüsselung

Verschlüsselung ist eine Massnahme oder ein Prozess, der es ermöglicht, Informationen mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unlesbare (d. h. nicht leicht interpretierbare) Zeichenfolge (Chiffretext) umzuwandeln.

## 6.1. Verschlüsselung während der Übertragung (Daten im Transit)

Die Frontify-Dienste sind nur auf Seiten mit HTTPS verfügbar, und HSTS-Header werden für alle Subdomains erstellt. Frontify nutzt Transport Layer Security (TLS) 1.2 (oder besser) für Daten, die über ein beliebiges Netzwerk übertragen werden. Frontify unterstützt die vollständige Verschlüsselung von Daten während der Übertragung. Keine nicht verschlüsselten Daten verlassen das Rechenzentrum. Alle Überwachungs- und Backend-Systeme senden entweder lokalen Datenverkehr über die VPC (Virtual Private Cloud) oder verwenden Verschlüsselung auf Transportebene, wenn sie mit dem Rest des Internets kommunizieren.

## 6.2. Verschlüsselung von ruhenden Daten (Daten im Ruhezustand)

Die Kundendaten werden in verschlüsselter Form in S3-Buckets gespeichert und logisch getrennt. Frontify verschlüsselt die Daten im Ruhezustand mit dem Advanced Encryption Standard (AES) 256-bit (oder besser).

# 7. Geheimhaltung

Frontify ergreift wirksame Massnahmen, um die Geheimhaltung der Daten zu gewährleisten und eine unbefugte Offenlegung von oder einen unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete Daten zu verhindern. Zu diesen Massnahmen gehören die physische Zugangskontrolle, die Einlasskontrolle, die Zugangskontrolle und die Trennungskontrolle.

## 7.1. Physische Zugangskontrolle

Massnahmen, die sicherstellen, dass Unbefugten der Zutritt zur Datenverarbeitungsinfrastruktur verwehrt wird.

Beschreibung des physischen Zugangskontrolle:

- kontrollierte Schlüsselverwaltung
- Türsicherung (elektronischer Türöffner)
- Überwachungssystem (Alarmanlage)
- Kontrollsystem für Besucher
- Hosting-Partner: Objektschutz, Zutritts- und Sicherheitspersonal
- Hosting-Partner: Schutz des Serverraums

## 7.2. Einlasskontrolle

Massnahmen, die sicherstellen, dass Unbefugte nicht auf die Daten zugreifen können.

Beschreibung der Einlasskontrolle:

- Passwortpolitik, d.h. persönliche und individuelle Benutzeranmeldung beim Zugriff auf das System (u.a. Sonderzeichen, Mindestlänge)
- Automatische Sperre (z. B. Passwort, Pausenmodus)
- Erstellung eines Benutzerstammsatzes pro Benutzer
- Begrenzung der Zahl der zugelassenen Mitarbeiter
- Verschlüsselung der Datenspeicherung
- Zugriffslisten
- Isolierung sensibler Systeme durch getrennte Netzbereiche
- Authentifizierungsverfahren (VPN, Zertifikate, Multi-Faktor-Authentifizierung)
- Protokollierung der Anmeldeversuche und Unterbrechung des Anmeldevorgangs nach einer bestimmten Anzahl erfolgloser Versuche

## 7.3. Zugangskontrolle

Massnahmen, die sicherstellen, dass die zum Zugriff auf eine Datenverarbeitungsinfrastruktur Berechtigten nur auf die Daten zugreifen können, die ihrer Zugriffsberechtigung unterliegen. Damit wird sichergestellt, dass Daten während der Verarbeitung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugangskontrolle:

- Konzept, das auf dem Prinzip der geringsten Rechte (Least Privilege Principle) beruht
- Berechtigungskonzepte (differenzierte Berechtigungen in Profilen, Rollen, etc.)
- Verschlüsselung von verschiedenen Datenspeichern

- Protokollierung von Zugriffen und Missbrauchsversuchen

### 7.4. Trennungskontrolle

Massnahmen, die sicherstellen, dass Daten, die für unterschiedliche Zwecke erhoben werden, getrennt von anderen Daten und Systemen verarbeitet und aufbewahrt werden, um eine ungeplante Nutzung dieser Daten für andere Zwecke auszuschliessen.

Beschreibung der Trennungskontrolle:

- Berechtigungskonzepte (differenzierte Berechtigungen in Profilen, Rollen, etc.)
- Verschlüsselte Speicherung von Daten
- Multi-Tenant-Umgebung mit logischer Kundentrennung
- Trennung von Test- und Produktivsystemen

## 8. Integrität

Massnahmen zur Wahrung der Integrität der Daten, um zu verhindern, dass Daten unbemerkt, unerlaubt oder ungewollt verändert werden. Zu diesen Massnahmen gehören Datenintegritätskontrolle, Übertragungskontrolle, Transportkontrolle und Eingabekontrolle.

### 8.1. Datenintegritätskontrolle

Massnahmen, die sicherstellen, dass Daten nicht durch Fehlfunktionen des Systems beschädigt oder geändert werden.

Beschreibung der Datenintegritätskontrolle:

- Implementierung von neuen Versionen und Patches mit einem Release/Patch-Management
- Betriebstest während der Implementierung und Releases/Patches durch die IT-Abteilung
- Protokollierung
- Transportprozesse mit individueller Verantwortung

### 8.2. Übertragungskontrolle

Massnahmen, die sicherstellen, dass überprüft und festgestellt werden kann, wohin Daten mit Hilfe von Datenübertragungseinrichtungen übermittelt wurden oder werden können.

Beschreibung der Übertragungskontrolle:

- Protokollierung
- Transportprozesse mit individueller Verantwortung
- Hashing

### 8.3. Transportkontrolle

Massnahmen, die sicherstellen, dass die Geheimhaltung und Integrität der Daten bei der Übermittlung von Daten und beim Transport von Datenträgern geschützt ist.

Beschreibung der Transportkontrolle:

- Übertragung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen (VPN)
- Transportprozesse mit individueller Verantwortung
- Verschlüsselungsverfahren, die Datenänderungen während des Transports erkennen
- Umfassende Protokollierungsverfahren

### 8.4. Eingabekontrolle

Massnahmen, die es ermöglichen, zu überprüfen und festzustellen, ob und von wem die Daten in der Datenverarbeitungsinfrastruktur eingegeben, geändert oder entfernt wurden.

Beschreibung der Eingabekontrolle:

- Protokollierung aller Systemaktivitäten und Aufbewahrung dieser Protokolle für mindestens ein Jahr
- Protokollanalysesysteme
- Hashing
- Digitale Signaturen

## 9. Erkennung und Verwaltung von Schwachstellen

Frontify nutzt Tools zur Erkennung von Sicherheitsrisiken, damit verdächtige Aktivitäten, potenzielle Schadprogramme, Viren und/oder bösartige Computercodes erkannt werden und Frontify darüber informiert wird.

Frontify scannt standardmässig alle Dateitypen auf Schadprogramme und setzt Massnahmen zur Eingabevalidierung ein, um die Ausführung von Programmen in Dateien zu verhindern, die vom Benutzer hochgeladen wurden und Schadprogramme enthalten. Darüber hinaus ermöglicht Frontify seinen Kunden, bestimmte Dateitypen zu einer Sperrliste hinzuzufügen.

Frontify hat ein Bug Bounty Programm eingeführt, um eine kontinuierliche Erkennung von Schwachstellen über das ganze Jahr hinweg zu gewährleisten.

Schwachstellen, die definierte Risikokriterien erfüllen, lösen automatische Sicherheitsmeldungen aus und werden entsprechend ihres Sicherheitsrisikos und ihrer Auswirkungen auf die Frontify-Dienste zur Behebung priorisiert.

## 10. Datenneutralität

Frontify überprüft die von den Kunden an die Frontify-Dienste gesendeten Daten nicht und verarbeitet alle Daten unabhängig von ihrer Art, sofern sie die vordefinierten Merkmale für die Verarbeitung erfüllen. Frontify trifft keine datenbasierten Entscheidungen, sondern führt nur die Anweisungen der Kunden aus, wenn diese die Inhalte in die Frontify-Dienste hochladen, um die gewünschten Resultate zu erzielen.

## 11. Administrative Massnahmen

Frontify überprüft im Rahmen seines Einstellungsverfahrens den strafrechtlichen Hintergrund seiner Angestellten, soweit dies in Anbetracht der Rolle des Angestellten angemessen und nach geltendem Recht zulässig ist.

Frontify führt regelmässig Schulungen zum Thema Datenschutz und Sicherheit durch und alle Angestellten müssen ein Onboarding-Programm absolvieren.

Die Angestellten von Frontify sind entweder durch ihren jeweiligen Arbeitsvertrag oder durch eine gesonderte Geheimhaltungsvereinbarung zur Geheimhaltung verpflichtet.

Die Angestellten von Frontify sind entweder durch ihren jeweiligen Arbeitsvertrag oder durch eine gesonderte Einwilligungserklärung zur Einhaltung der Informationssicherheitsrichtlinien verpflichtet.

## 12. Verfügbarkeit und Belastbarkeit

Massnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit von Datenverarbeitungsanlagen, um zu gewährleisten, dass hohe Belastungen oder starke Dauerbelastungen bewältigt werden können und dass der Zugriff auf die Daten bei einem physischen oder technischen Zwischenfall zeitnah wiederhergestellt wird. Zu

diesen Massnahmen gehören die Verfügbarkeitskontrolle, die zeitnahe Wiederherstellung der Verfügbarkeit und die Zuverlässigkeit.

## 12.1. Verfügbarkeitskontrolle

Massnahmen, die sicherstellen, dass die Daten vor versehentlicher Zerstörung oder Verlust geschützt sind.

Beschreibung der Verfügbarkeitskontrolle:

- Hosting-Partner: Verfahren zur Datensicherung
- Hosting-Partner: Unterbrechungsfreie Stromversorgung
- Hosting-Partner: Brandmeldeanlage
- Hosting-Partner: Klimatisierung
- Hosting-Partner: Alarmanlage
- Hosting-Partner: Notfallpläne
- Hosting-Partner: Keine wasserführenden Leitungen über oder neben den Serverräumen

## 12.2. Zeitnahe Wiederherstellung der Verfügbarkeit

Massnahmen, die sicherstellen, dass die Verfügbarkeit von und der Zugang zu den Daten im Falle eines physischen oder technischen Zwischenfalls zeitnah wiederhergestellt wird.

Beschreibung der zeitnahen Wiederherstellung der Verfügbarkeit:

- Datensicherungsverfahren
- Regelmässige Tests der Datenwiederherstellung
- Katastrophen- und Notfallpläne
- Off-Site-Backup
- Hosting-Partner: Verfügbarkeitszonen

## 12.3. Zuverlässigkeit

Massnahmen, die sicherstellen, dass alle Funktionen des Systems verfügbar sind und dass etwaige Störungen gemeldet werden.

Beschreibung der Zuverlässigkeit:

- Automatische Überwachung mit E-Mail-Benachrichtigung
- Katastrophen- und Notfallpläne mit Zuständigkeiten
- Regelmässige Tests der Datenwiederherstellung

Frontify

# 13. Meldung von Sicherheitsvorfällen

Wenn Frontify von einem Sicherheitsvorfall Kenntnis erlangt, der zur versehentlichen oder unrechtmässigen Zerstörung, Verlust, Änderung, Offenlegung oder Zugriff der personenbezogenen Daten des Kunden führt, benachrichtigt Frontify die betroffenen Kunden unverzüglich in Übereinstimmung mit seinen vertraglichen Verpflichtungen und den Anforderungen der anwendbaren Datenschutzgesetze. Zudem ergreift Frontify unverzüglich angemessene Massnahmen, um den Sicherheitsvorfall einzudämmen, zu untersuchen und zu beheben.

# 14. Regelmässige Überprüfung, Bewertung und Evaluierung

Frontify hat ein Verfahren implementiert, um die Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmässig zu prüfen, zu bewerten und zu evaluieren. Dazu gehören ein Bewertungsverfahren und eine Vertragskontrolle.

## 14.1. Bewertungsverfahren

Massnahmen, die gewährleisten, dass die Daten sicher und im Einklang mit den Datenschutzbestimmungen verarbeitet werden.

Beschreibung des Bewertungsverfahrens:

- Datenschutzmanagement
- Formalisierte Verfahren für Datenschutzvorfälle
- Dokumentation der Anweisungen der Kunden
- Formalisierte Auftragsverwaltung
- Service Level Agreements

## 14.2. Vertragskontrolle

Massnahmen, die sicherstellen, dass die Daten gemäss den Anweisungen des Kunden verarbeitet werden.

Beschreibung der Vertragskontrolle:

- Klare Vertragsformulierung
- Dokumentation der Anweisungen der Kunden
- Formalisierte Auftragsverwaltung

Frontify