



RECHTSTEXTE

Auftragsverarbeitungsvertrag

Anlage 1 zu den Allgemeinen Geschäftsbedingungen

Version 2.0 · gültig ab 01.11.2026

Structify Solutions UG (haftungsbeschränkt) · Gartenstraße 8 · 92348 Berg · Amtsgericht Nürnberg HRB 46012
Maßgeblich ist die unter structify.solutions/rechtliches veröffentlichte Fassung. Bei Abweichungen zwischen der deutschen und der englischen Fassung geht die deutsche Fassung vor.

Auftragsverarbeitungsvertrag

Anlage 1 zu den Allgemeinen Geschäftsbedingungen der Structify Solutions UG (haftungsbeschränkt)

Version 2.0 · gültig ab 01.11.2026

Präambel – Parteien und Abschluss

(1) Dieser Auftragsverarbeitungsvertrag (AVV) gilt zwischen dem Kunden als Verantwortlichem im Sinne des Art. 4 Nr. 7 DSGVO (nachfolgend „Verantwortlicher“) und der Structify Solutions UG (haftungsbeschränkt), Gartenstraße 8, 92348 Berg, Amtsgericht Nürnberg HRB 46012, als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO (nachfolgend „Structify“).

(2) Der Verantwortliche ist Unternehmer im Sinne des § 14 BGB oder eine juristische Person des öffentlichen Rechts.

(3) Dieser AVV ist Anlage und Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) von Structify. Er wird mit deren Annahme durch eine vertretungsberechtigte Person des Verantwortlichen in Textform geschlossen; dieses elektronische Format erfüllt Art. 28 Abs. 9 DSGVO. Eine gesonderte Unterschrift ist nicht nötig. Structify protokolliert Zeitpunkt und Version der Annahme. Der AVV ist unter structify.solutions/rechtliches/avv jederzeit abrufbar und speicherbar.

(4) Haben die Parteien einen individuellen Auftragsverarbeitungsvertrag geschlossen, geht dieser vor (§ 11).

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen bei der Bereitstellung der Produkte Structify Web, Structify Desktop, Structify Mobile und Structify Operate sowie der zugrunde liegenden Plattform (nachfolgend gemeinsam „Plattform“) nach dem Vertrag, den die Parteien auf Grundlage der AGB geschlossen haben (nachfolgend „Hauptvertrag“).

(2) Der AVV beginnt mit dem Hauptvertrag und endet mit ihm, ohne dass es einer Kündigung bedarf. Pflichten zu Löschung, Rückgabe und Vertraulichkeit gelten über das Vertragsende hinaus.

§ 2 Art, Zweck und Ort der Verarbeitung

(1) Art und Zweck der Verarbeitung, die Datenarten und die Kategorien betroffener Personen beschreibt Anlage 1 dieses AVV je Produkt.

(2) Hosting und Speicherung der Plattformdaten erfolgen in Deutschland (EU). Für KI-Auswertungen (Sprache, Text, Bilder) setzt Structify US-Anbieter ein (OpenAI, Anthropic); weitere Dienstleister mit Drittlandbezug nennt Anlage 3. Übermittlungen in Drittländer erfolgen nur nach § 8.

§ 3 Pflichten von Structify (Art. 28 Abs. 3 DSGVO)

Structify

- a) verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch bei Übermittlungen in Drittländer, sofern Structify nicht durch Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet ist; in diesem Fall teilt Structify dem Verantwortlichen diese Pflicht vorher mit, soweit das Recht es nicht verbietet. Hält Structify eine Weisung für rechtswidrig, informiert Structify den Verantwortlichen unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen;
- b) stellt sicher, dass alle Personen, die die Daten verarbeiten dürfen, zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen, auch über ihre Tätigkeit hinaus;
- c) trifft alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen nach

Anlage 2 und entwickelt sie nach dem Stand der Technik fort, ohne das vereinbarte Schutzniveau zu unterschreiten;

d) hält die Bedingungen für Unterauftragsverarbeiter nach § 5 ein;

e) unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO), insbesondere durch Auskunft-, Berichtigungs-, Löscho- und Exportfunktionen, und leitet Anträge, die bei Structify eingehen, unverzüglich an den Verantwortlichen weiter;

f) unterstützt den Verantwortlichen bei den Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Meldungen von Datenschutzverletzungen, der Benachrichtigung Betroffener, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen;

g) löscht nach Ende der Leistungen alle personenbezogenen Daten oder stellt sie zum Export bereit, soweit keine Speicherpflicht besteht (§ 10);

h) stellt alle Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO bereit und ermöglicht Überprüfungen nach § 7.

§ 4 Weisungen

(1) Dieser AVV und der Hauptvertrag sind die dokumentierte Weisung. Die vertragsgemäße Nutzung der Plattformfunktionen durch den Verantwortlichen, seine Nutzer und die von ihm eingeladenen Externen gilt als Weisung zur entsprechenden Verarbeitung. Das umfasst auch Übermittlungen, die der Verantwortliche selbst auslöst, etwa an Kalender- oder Speicherdienste in seinen eigenen Konten, an Projektbeteiligte oder per E-Mail. Das gilt auch für die Kartenanzeige des Aufnahmeorts von Fotos: Der Kartenausschnitt der OpenStreetMap Foundation wird erst geladen, wenn ein Nutzer ihn ausdrücklich anfordert („Karte laden“); sein Browser ruft die Karte dann direkt bei der OpenStreetMap Foundation ab, die dabei eigenständig verantwortlich und kein Unterauftragsverarbeiter ist.

(2) Der Verantwortliche ist für die Zulässigkeit der Verarbeitung und die Rechte der Betroffenen verantwortlich. Das umfasst die Information betroffener Personen, etwa wenn Beschäftigte oder Dritte auf Fotos oder in Sprachaufnahmen erfasst werden oder Standortdaten zu Aufnahmen gespeichert werden.

(3) Einzelweisungen erteilt der Verantwortliche in Textform, etwa per E-Mail an support@structify.solutions; mündliche Weisungen bestätigt er unverzüglich in Textform. Weisungsberechtigt sind die gesetzlichen Vertreter des Verantwortlichen, die von ihnen in Textform benannten Personen und die Nutzer mit der Rolle Geschäftsführung.

(4) Verlangt eine Einzelweisung Leistungen über den vertraglichen Umfang hinaus, kann Structify eine angemessene Vergütung des Mehraufwands verlangen, wenn Structify vorher darauf hinweist.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt Structify die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen (Art. 28 Abs. 2 DSGVO). Die eingesetzten Unterauftragsverarbeiter nennt Anlage 3; die aktuelle Liste steht unter structify.solutions/rechtliches.

(2) **Vorabinformation.** Structify informiert den Verantwortlichen **mindestens 30 Tage vorher** in Textform über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Die Information nennt Namen, Sitz, Leistung, Datenstandort und die Grundlage einer etwaigen Drittlandübermittlung.

(3) **Widerspruch.** Der Verantwortliche kann der Änderung **innerhalb von 14 Tagen nach Zugang** der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Widerspricht er nicht fristgerecht, gilt die Änderung als genehmigt; Structify weist in der Information auf Frist und Folge hin.

(4) Widerspricht der Verantwortliche berechtigt, suchen die Parteien eine einvernehmliche Lösung, etwa den Verzicht auf den neuen Unterauftragsverarbeiter für diesen Verantwortlichen. Gelingt das nicht, kann

der Verantwortliche den Hauptvertrag zum Zeitpunkt der Änderung kündigen; bereits bezahlte Entgelte für die Zeit danach erstattet Structify anteilig.

(5) **Dringende Fälle.** Muss Structify einen Unterauftragsverarbeiter kurzfristig ersetzen, weil dieser seine Leistung einstellt oder ein erhebliches Sicherheitsrisiko besteht, kann die Frist nach Absatz 2 kürzer sein. Structify informiert dann unverzüglich; das Widerspruchs- und Kündigungsrecht nach Absatz 3 und 4 bleibt bestehen.

(6) Structify erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf wie dieser AVV (Art. 28 Abs. 4 DSGVO) und haftet gegenüber dem Verantwortlichen für deren Einhaltung.

§ 6 Meldung von Datenschutzverletzungen

(1) Structify meldet dem Verantwortlichen jede Verletzung des Schutzes der im Auftrag verarbeiteten Daten unverzüglich nach Bekanntwerden. Die Meldung enthält, soweit verfügbar, die Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben liefert Structify schrittweise ohne unangemessene Verzögerung nach.

(2) Structify unterstützt den Verantwortlichen bei den Pflichten aus Art. 33 und 34 DSGVO und dokumentiert jede Verletzung. Die Bewertung der Meldepflicht, die Meldung an die Aufsichtsbehörde und die Benachrichtigung Betroffener obliegen dem Verantwortlichen.

§ 7 Kontrollen

(1) Der Verantwortliche kann sich vor Beginn und während der Verarbeitung von der Einhaltung dieses AVV überzeugen. Den Nachweis erbringt Structify vorrangig durch aktuelle Selbstauskünfte, Berichte unabhängiger Stellen, soweit vorhanden, und Nachweise der Unterauftragsverarbeiter.

(2) Soweit erforderlich, ermöglicht Structify Prüfungen vor Ort durch den Verantwortlichen oder einen zur Verschwiegenheit verpflichteten Prüfer, der kein Wettbewerber von Structify ist, nach angemessener Ankündigung in Textform, zu üblichen Geschäftszeiten, ohne unverhältnismäßige Störung und unter Wahrung von Geschäftsgeheimnissen und Daten anderer Kunden.

(3) Jede Partei trägt ihre Kosten selbst. Für anlasslose Prüfungen, die häufiger als einmal im Kalenderjahr stattfinden, kann Structify eine angemessene Vergütung verlangen; Prüfungen aus konkretem Anlass bleiben davon unberührt.

§ 8 Übermittlung in Drittländer

(1) Hosting und Speicherung der Plattformdaten erfolgen in Deutschland (EU): die Datenbank und die Dateiablagen im Rechenzentrum Frankfurt am Main, die verschlüsselten Sicherungskopien im Rechenzentrum Falkenstein.

(2) Eine Übermittlung in ein Land außerhalb der EU und des Europäischen Wirtschaftsraums (Drittland) erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Grundlage für alle Unterauftragsverarbeiter mit Drittlandbezug sind die **Standardvertragsklauseln der Europäischen Kommission** nach Art. 46 Abs. 2 lit. c DSGVO (Durchführungsbeschluss (EU) 2021/914), **Modul 3** (Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter). Datenexporteur ist Structify, Datenimporteur der jeweilige Unterauftragsverarbeiter. Structify gibt Weisungen des Verantwortlichen an den Unterauftragsverarbeiter weiter.

(3) Ist ein Unterauftragsverarbeiter nach dem EU-U.S. Data Privacy Framework zertifiziert (Angemessenheitsbeschluss (EU) 2023/1795), gibt Anlage 3 dies ergänzend an. Die Zertifizierung ersetzt die Standardvertragsklauseln nicht; entfällt sie, bleiben die Standardvertragsklauseln maßgeblich. Structify prüft die Angaben mindestens jährlich im offiziellen Register.

(4) Für jeden Unterauftragsverarbeiter mit Drittlandbezug hat Structify die Folgen der Übermittlung abgeschätzt (Klausel 14 der Standardvertragsklauseln) und ergänzende Maßnahmen festgelegt, insbesondere Transportverschlüsselung, den vertraglichen Ausschluss des Trainings von KI-Modellen mit Inhalten, die Begrenzung der Speicherdauer beim Unterauftragsverarbeiter, die Wahl einer Verarbeitungsregion in der EU, soweit verfügbar, und Datenminimierung. Die Abschätzung wird mindestens jährlich und bei wesentlichen Änderungen überprüft.

(5) Auf Anfrage erhält der Verantwortliche eine Kopie der Standardvertragsklauseln und eine Zusammenfassung der Abschätzung; Geschäftsgeheimnisse und Sicherheitsdetails können unkenntlich gemacht werden.

§ 9 Kein KI-Training, anonymisierte Statistik

(1) Structify hat mit allen KI-Anbietern vertraglich vereinbart, dass sie Inhalte des Verantwortlichen nicht zum Training von KI-Modellen verwenden.

(2) Structify selbst verwendet Inhalte des Verantwortlichen nicht zum Training von KI-Modellen, es sei denn, der Verantwortliche hat nach § 14 Abs. 2 der AGB ausdrücklich eingewilligt. Eine solche Einwilligung ist eine Weisung im Sinne des § 4; sie kann jederzeit widerrufen werden.

(3) **Anonymisierte Nutzungsstatistik.** Der Verantwortliche weist Structify an, Nutzungsereignisse (welche Funktion wann genutzt wurde, Zeitstempel und technische Kennzahlen) ohne Inhalte zu anonymen, zusammengefassten Statistiken zu verdichten. Structify darf diese anonymen Statistiken für eigene Zwecke nutzen, nämlich zur Verbesserung der Produkte, zur Sicherung des Betriebs, zur Kapazitätsplanung und zum Beleg eigener Leistungsangaben. Die Anonymisierung erfolgt so, dass ein Personenbezug und ein Bezug zum einzelnen Verantwortlichen nicht mehr herstellbar sind; Rohdaten mit Personenbezug werden nach der Verdichtung gelöscht, spätestens nach 90 Tagen. Nach der Anonymisierung unterliegen die Statistiken nicht mehr diesem AVV.

§ 10 Laufzeit, Vertragsende und Löschung

(1) Nach Ende des Hauptvertrags haben die bisherigen Nutzer des Verantwortlichen **30 Tage lang lesenden Zugang**, um Daten anzusehen und zu exportieren (§ 25 AGB). Der Export in gängigen, maschinenlesbaren Formaten ist die Rückgabe der Daten im Sinne des Art. 28 Abs. 3 lit. g DSGVO. Eine andere Form der Rückgabe kann der Verantwortliche gegen Erstattung des Aufwands verlangen.

(2) Nach Ablauf der 30 Tage löscht Structify alle im Auftrag verarbeiteten personenbezogenen Daten. Auf Weisung löscht Structify früher. Auf Verlangen bestätigt Structify die Löschung in Textform.

(3) Aus Sicherungskopien werden Daten nicht einzeln entfernt. Sie laufen mit dem jeweiligen Sicherungsstand aus, in der Datenbank spätestens nach sechs Monaten, in den Dateiablagen nach 90 Tagen (Anlage 2 Nr. 3), und sind bis dahin gegen jede weitere Verarbeitung geschützt. Die Löschbestätigung weist darauf hin.

(4) Daten, die Structify nach Unionsrecht oder dem Recht eines Mitgliedstaats aufbewahren muss, schränkt Structify in der Verarbeitung ein und löscht sie nach Ablauf der Frist.

(5) Die Vertraulichkeitspflichten gelten über das Vertragsende hinaus.

§ 11 Haftung und Rangfolge

(1) Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für den Teil des Schadens, der auf ihre Verletzung der DSGVO oder dieses AVV zurückgeht. Im Übrigen gelten die Haftungsregeln der AGB, soweit zwingendes Recht nicht entgegensteht.

(2) In Fragen des Datenschutzes geht dieser AVV den AGB, den Nutzungsbedingungen und sonstigen Vereinbarungen vor. Ein individueller Auftragsverarbeitungsvertrag zwischen den Parteien geht diesem AVV vor. Zwingendes Recht, insbesondere die DSGVO, geht allen vertraglichen Regeln vor.

§ 12 Verantwortliche in der Schweiz

Hat der Verantwortliche seinen Sitz in der Schweiz oder unterliegt die Verarbeitung dem Schweizer Datenschutzgesetz (DSG), gilt ergänzend:

- a) Verweise auf die DSGVO umfassen die entsprechenden Bestimmungen des DSG.
- b) Zuständige Aufsichtsbehörde für Verarbeitungen nach dem DSG ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).
- c) Deutschland und die EU gelten nach Schweizer Recht als Staaten mit angemessenem Datenschutz. Für Übermittlungen in Drittländer gelten die Standardvertragsklauseln nach § 8 mit den vom EDÖB anerkannten Anpassungen für die Schweiz.
- d) Der Begriff „Mitgliedstaat“ in den Standardvertragsklauseln umfasst die Schweiz, damit betroffene Personen mit gewöhnlichem Aufenthalt in der Schweiz ihre Rechte dort geltend machen können.

Für Verantwortliche in Liechtenstein gilt die DSGVO unmittelbar; zuständig ist die Datenschutzstelle Liechtenstein.

§ 13 Schlussbestimmungen

- (1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts, auch für Verantwortliche mit Sitz in Österreich, der Schweiz oder Liechtenstein; zwingendes Datenschutzrecht am Sitz des Verantwortlichen bleibt unberührt.
- (2) Änderungen dieses AVV erfolgen nach dem Verfahren für Änderungen der AGB (§ 26 AGB). Für neue oder ersetzte Unterauftragsverarbeiter gilt zusätzlich § 5.
- (3) Der AVV liegt auf Deutsch und Englisch vor; bei Abweichungen geht die deutsche Fassung vor.
- (4) Ist eine Bestimmung unwirksam, bleiben die übrigen wirksam; an ihre Stelle treten die gesetzlichen Vorschriften, insbesondere die DSGVO.

Anlage 1 – Beschreibung der Verarbeitung je Produkt

A. Gemeinsam für alle Produkte

Art der Verarbeitung: Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung an vom Verantwortlichen bestimmte Empfänger, Abgleichen, Einschränken, Löschen.

Kategorien betroffener Personen:

- Beschäftigte und sonstige Nutzer des Verantwortlichen;
- Externe, die der Verantwortliche einlädt (etwa ausführende Unternehmen, Subunternehmer, Bauherren, Bieter, Fachplaner, Zuschauer);
- Ansprechpersonen von Auftraggebern, Behörden, Lieferanten und Dienstleistern;
- Personen, die auf Fotos, Videos oder Sprachaufnahmen erfasst oder in Dokumenten genannt sind.

Allgemeine Datenarten: Stammdaten der Nutzer (Name, E-Mail-Adresse, Rolle, Funktion), Kontaktdaten von Beteiligten, Kommunikations- und Protokollinhalte, Nutzungs- und Protokolldaten (Anmeldezeitpunkte, IP-Adressen bei Sicherheitsereignissen, technische Protokolle).

B. Structify Web und Structify Desktop

Zweck: Projektsteuerung und Projektdokumentation für Planung und Bau, insbesondere Projekt- und Aufgabenorganisation, Kontakt- und Kundenverwaltung (CRM), Tickets, Mängel und Abnahmen, Plan- und Dokumentenverwaltung, Bautagebuch und Baustellendokumentation mit Foto-, Video- und Audioaufnahmen und deren Transkription, begehbare 3D-Rundgänge aus Begehungsvideos, Ausschreibung und Vergabe einschließlich Bieterportal, Termine und Kalender, Zeiterfassung, Honorarermittlung, Rechnungsstellung und Mahnwesen, E-Mail- und Benachrichtigungsversand, elektronische Signatur, Schnittstellen (API, MCP, CLI, Webhooks, Kalender-Feeds) sowie KI-gestützte Funktionen (Assistent „KAI“, Auswertungen, Vorschläge).

Datenarten zusätzlich: Projekt-, Bau- und Mängeldaten; Foto-, Video- und Audiomaterial und Transkripte; Standortangaben zu Fotos, soweit vorhanden; Plan- und Dokumentinhalte; Angebots- und Vergabedaten von Bietern; Abrechnungs- und Honorardaten mit Personenbezug; Signaturdaten der Unterzeichnenden.

Structify Desktop greift auf dieselben Daten zu wie Structify Web; lokal speichert die Desktop-App nur Sitzungsdaten (die Anmeldung verschlüsselt im Schlüsselbund des Betriebssystems), Einstellungen sowie vorübergehend nicht abgeschlossene Eingaben wie Entwürfe und technische Angaben zu noch nicht abgeschlossenen Uploads.

C. Structify Mobile

Zweck: Erfassung auf der Baustelle und an Anlagen (Begehungen, Sprachnotizen, Diktate, Fotos, Tickets, Mängel, Abnahmen, Aufmaße), Synchronisation mit der Plattform, Auswertung durch KI-Funktionen, Anmeldung per Geräte-Kopplung.

Datenarten zusätzlich: Fotos einschließlich Metadaten (Aufnahmezeit, Gerätemodell, Standort, soweit freigegeben); Sprachaufnahmen und Transkripte; Standort zum Zeitpunkt einer Aufnahme (nur bei Freigabe, nicht im Hintergrund); Geräteerkennung als Hashwert, Plattformbezeichnung und Zeitpunkte der Kopplung.

Besonderheit: Ohne Netzverbindung erfasste Daten hält die App bis zur Übertragung lokal auf dem Gerät vor und löscht sie nach erfolgreicher Übertragung. Lokale Daten unterliegen dem Schutz des Geräts; Structify sichert sie nicht.

D. Structify Operate

Zweck: digitales Betriebstagebuch für Betreiber technischer Anlagen, etwa Heizwerke, Wärmenetze, Biomasse- und Versorgungsanlagen: Betriebs- und Tagebucheinträge, Wartungen und Fristen, Störungen und Tickets, Einsatzstoffe, Lieferungen und Bestellungen, Komponenten mit Einbau- und Austauschhistorie, Zählerstände und Messwerte, Nachweise, Berichte und Prüf-Exporte, Benachrichtigungen bei Fristen und Auffälligkeiten, Rollen Admin, Anwender und Zuschauer sowie KI-gestützte Funktionen (Assistent „KAI“, Auswertungen von Betriebs- und Messdaten, Berechnungen, Empfehlungen etwa zu Wartung, Bestellungen und Verbrauch, Berichte, Texterkennung aus Fotos von Zählern, Lieferscheinen und Rechnungen, Transkription von Sprachnotizen und Schichtübergaben).

Datenarten zusätzlich: Namen und Rollen der Personen, die Einträge anlegen, prüfen oder freigeben, mit Zeitstempel; Angaben zur Rufbereitschaft und zu Benachrichtigungseinstellungen (Name, E-Mail-Adresse, Telefonnummer, gewählte Benachrichtigungsarten); Schichtbuch- und Übergabeinhalte; Angaben zu Wartungs- und Prüfdienstleistern sowie Lieferanten und deren Ansprechpersonen (etwa Lieferant, Fahrzeug, Menge, Zeitpunkt); Fotos und Dokumente zu Anlagen, Störungen, Lieferungen und Rechnungen; Sprachaufnahmen und Transkripte.

Besonderheit: Structify Operate läuft auf derselben Plattform wie die übrigen Produkte (Datenbank und Dateiablagen in Frankfurt am Main, § 8 Abs. 1). Die KI-Funktionen nutzen die in Anlage 3 genannten KI-Anbieter (Anthropic; für die Transkription OpenAI). Structify Operate gibt keine Steuerbefehle an Anlagen

aus und greift nicht in deren Betrieb ein; Empfehlungen der KI werden erst nach Prüfung und Freigabe durch eine berechtigte Person umgesetzt. Ausgenommen sind automatische Benachrichtigungen nach festen Regeln, etwa bei Überschreitung eingestellter Grenzwerte oder bei unbearbeiteten Störungen: Structify Operate legt dabei ohne vorherige Freigabe Tickets an, kennzeichnet sie als „eskaliert“ und benachrichtigt die vom Verantwortlichen dafür eingetragenen Personen in der Anwendung und per E-Mail; die KI formuliert dabei nur Erläuterungen und Nachrichtentexte, sie entscheidet nicht über die Auslösung. Zuschauer haben nur lesenden Zugriff im vom Admin freigegebenen Umfang.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Structify trifft insbesondere die folgenden Maßnahmen und entwickelt sie nach dem Stand der Technik fort.

1. Vertraulichkeit

- **Zutritt:** Betrieb ausschließlich in Rechenzentren der in Anlage 3 genannten Anbieter mit physischer Zutrittskontrolle (Frankfurt am Main, Falkenstein); Structify betreibt keine eigenen Serverräume.
- **Zugang:** Anmeldung nur nach Authentifizierung. Für die Nutzerkonten des Verantwortlichen ist die Zwei-Faktor-Authentifizierung verpflichtend (Einmalcodes nach TOTP oder Sicherheitsschlüssel und Passkeys nach dem WebAuthn-Standard). Ausgenommen sind Test- und Demozugänge bis zum Ende der Testphase sowie ein Prüfzugang mit fiktiven Daten für die App-Store-Prüfung. Die zwei Konten der Plattformadministration von Structify melden sich ohne zweiten Faktor an; jede Anmeldung wird serverseitig protokolliert und den Administratoren gemeldet; dauerhaftes Geräte-Vertrauen setzt einen zweiten Faktor voraus. Schutz der Anmeldung vor automatisierten Angriffen. Geräte-Kopplung per einmalig einlösbarem QR-Code (5 Minuten gültig); Geräte-Vertrauen höchstens 30 Tage, bei Test- und Demozugängen höchstens bis zum Testende, jederzeit widerrufbar.
- **Zugriff:** Mandantentrennung auf Datenbankebene (Row Level Security): jede Organisation sieht nur eigene Daten; rollenbasiertes Berechtigungskonzept innerhalb der Organisation; Zugriff nur für Projektmitglieder; administrative Zugriffe von Structify nur nach dem Erforderlichkeitsprinzip und protokolliert.
- **Trennung:** getrennte Verarbeitung von Test-, Showroom- und Produktivdaten durch getrennte Organisationen.

2. Integrität

- **Eingabekontrolle:** Protokollierung sicherheitsrelevanter Vorgänge; unveränderliche Prüfprotokolle für abrechnungs- und aufbewahrungsrelevante Vorgänge.
- **Weitergabekontrolle:** Übertragung nur über verschlüsselte Verbindungen (TLS); Anbindung externer Dienste nur über authentifizierte Schnittstellen.

3. Verfügbarkeit, Belastbarkeit und Wiederherstellung

- Betrieb der Datenbank im Rechenzentrum Frankfurt am Main.
- Sicherung der Datenbank stündlich; Vorhaltung gestuft: stündliche Stände 48 Stunden, tägliche 35 Tage, wöchentliche 12 Wochen, monatliche 6 Monate. Dateiablagen werden stündlich gespiegelt; gelöschte oder überschriebene Dateien bleiben 90 Tage erhalten.
- Zusätzlich erstellt der Hosting-Anbieter der Datenbank täglich eine eigene Sicherung und hält sie sieben Tage vor.
- Wiederhergestellt wird auf einen vorhandenen Sicherungsstand, in der Regel den jüngsten stündlichen. Eine minutengenaue Wiederherstellung auf einen beliebigen Zeitpunkt wird nicht angeboten.
- Zweiter, getrennter Sicherungsstandort im Rechenzentrum Falkenstein (Hetzner Online GmbH): Die Sicherungen werden auf einem von Structify verwalteten Server erzeugt (Zugang nur per SSH-

Schlüssel, Firewall, automatische Sicherheitsaktualisierungen) und verschlüsselt abgelegt (Datenbank: BorgBackup mit AES; Dateiablagen: rclone crypt mit AES einschließlich Datei- und Ordernamen). Auf dem Speicher liegen nur verschlüsselte Daten; die Schlüssel verbleiben bei Structify. Zusätzlich tägliche Momentaufnahmen des Sicherungsspeichers.

- Wöchentliche automatische Prüfung der Sicherungen auf Vollständigkeit und Lesbarkeit; automatische Alarmierung der Geschäftsführung bei ausbleibenden oder fehlgeschlagenen Läufen.
- Wiederherstellungsübungen vierteljährlich; erste Übungen am 26. und 27.09.2026 mit vollständiger Wiederherstellung der Datenbank und der Dateiablagen in eine isolierte Umgebung.
- **Wiederherstellungszeiten (zugesichert, ab Kenntnis des Verlusts):** Teilverlust (einzelne Datensätze, Tabellen, Dateien) höchstens 2 Stunden; Totalverlust (Datenbank oder Anbieterkonto) höchstens 8 Stunden bis zur erneuten Nutzbarkeit im Webbrowser. Angestrebter maximaler Datenverlust: eine Stunde. Ausgenommen sind über App-Stores vertriebene Apps, die nach einem Totalverlust eine neue, vom Store-Betreiber zu prüfende Version benötigen, sowie Zeiten, in denen ein Infrastruktur-Anbieter selbst großflächig nicht verfügbar ist.
- Löschungen wirken in Sicherungskopien mit deren Auslaufen (spätestens sechs Monate); bei einer Wiederherstellung werden zuvor gelöschte Daten nicht reaktiviert.

4. Verschlüsselung

- Transportverschlüsselung (TLS) für alle Verbindungen.
- Verschlüsselung gespeicherter Daten bei den Hosting-Anbietern.

5. Überprüfung und Weiterentwicklung

- regelmäßige interne Sicherheitsprüfungen, insbesondere der Zugriffsregeln und der Mandantentrennung;
- automatisierte Prüfungen, die zentrale Sicherheitsvorgaben (u. a. Zugriffsregeln auf Datenbankebene) vor jeder Auslieferung kontrollieren;
- Anpassung der Maßnahmen anhand der Ergebnisse.

6. Unterauftragsverarbeiter

- Auswahl nach Datenschutz- und Sicherheitsniveau; Verträge nach Art. 28 DSGVO; bei Drittlandbezug Standardvertragsklauseln und Abschätzung der Übermittlungsfolgen (§ 8); vertraglicher Ausschluss des KI-Trainings bei KI-Anbietern.

Anlage 3 – Unterauftragsverarbeiter

Übermittlungsgrundlage. Soweit ein nachstehend genannter Unterauftragsverarbeiter Daten in einem Drittland verarbeitet oder ein Zugriff aus einem Drittland nicht ausgeschlossen werden kann, stützt Structify die Übermittlung auf die Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/914), **Modul 3** (Structify als Auftragsverarbeiter an den Unterauftragsverarbeiter), mit einer dokumentierten Abschätzung der Übermittlungsfolgen (§ 8). Eine Zertifizierung nach dem EU-U.S. Data Privacy Framework ist bei allen zertifizierten Anbietern ergänzend angegeben; Grundlage bleiben die Standardvertragsklauseln und die Abschätzung. Stand der Prüfung: 28.09.2026. Verarbeitungen, für die Structify selbst Verantwortlicher ist (etwa Website, Schutz der Anmeldung, eingebundene Inhalte, Ansprache potenzieller Kunden), sind keine Auftragsverarbeitung für den Verantwortlichen; sie und die dafür geltenden Standardvertragsklauseln (Modul 2) beschreibt die Datenschutzerklärung.

Ständig eingesetzt

Unterauftragsverarbeiter	Leistung	Datenstandort	Drittland und Grundlage
Supabase Pte. Ltd., Singapur	Datenbank, Anmeldung, Dateispeicher, Server-Funktionen (Hosting der Plattformdaten)	Frankfurt am Main, Deutschland	Vertragspartner in Singapur; Support- oder Konzernzugriff aus Singapur oder den USA nicht ausgeschlossen. SCC Modul 3; kein DPF
Vercel Inc., USA	Hosting und Auslieferung der Webanwendung	Auslieferung über Frankfurt am Main; Verarbeitung auch in den USA möglich	USA. SCC Modul 3; ergänzend DPF-zertifiziert
Hetzner Online GmbH, Gunzenhausen, Deutschland	Datensicherung: Erzeugung und Ablage ausschließlich verschlüsselter Sicherungskopien	Falkenstein, Deutschland	kein Drittland
Anthropic PBC, USA (Vertragspartner im EWR: Anthropic Ireland, Limited)	KI-Auswertung von Text, Bildern und Dokumenten, Assistent „KAI“, Vorschläge; in Structify Operate zusätzlich Auswertungen, Berechnungen und Empfehlungen	USA	USA. SCC Modul 3; kein DPF
OpenAI, L.L.C., USA (Vertragspartner im EWR: OpenAI Ireland Ltd.)	Transkription von Sprachaufnahmen, auch in Structify Operate	USA	USA. SCC Modul 3; kein DPF
Plus Five Five, Inc. („Resend“), USA	Versand von System- und Benachrichtigungs-E-Mails	USA	USA. SCC Modul 3; ergänzend DPF-zertifiziert
RunPod, Inc., USA	Rechenleistung für begehbare 3D-Rundgänge aus Begehungsvideos; abgebildete Personen werden vorher automatisiert unkenntlich gemacht	EU-Region der Secure Cloud	US-Rechtsträger. SCC Modul 3; kein DPF
Oneflow AB, Stockholm, Schweden	elektronische Signatur von Dokumenten einschließlich der Daten der Unterzeichnenden	EU (Irland, Sicherung Schweden)	kein Drittland
IONOS SE, Montabaur, Deutschland	E-Mail-Postfächer von Structify für die Kommunikation mit Kunden, etwa Support per E-Mail	Deutschland	kein Drittland

Nur bei Nutzung der jeweiligen Funktion

Unterauftragsverarbeiter	Leistung	Datenstandort	Drittland und Grundlage
Cal.com, Inc., USA	Terminbuchung für Gespräche mit Structify aus der Anwendung	USA	USA. SCC Modul 3; kein DPF

Keine Unterauftragsverarbeiter

- **Stripe** (Stripe Payments Europe, Ltd., Irland) wickelt Zahlungen als eigenständig Verantwortlicher ab. Kartendaten werden nicht in der Plattform gespeichert.
- Dienste, die der Verantwortliche selbst verbindet und an die er Daten in **eigene Konten** übermittelt (etwa Kalenderdienste oder eigene Code- und Speicherablagen), handeln nicht als Unterauftragsverarbeiter von Structify; die Übermittlung erfolgt auf Weisung des Verantwortlichen (§ 4 Abs. 1).
- Dienste, bei denen Structify selbst Verantwortlicher ist (etwa der Hilfe-Sprachassistent im Hilfebereich der Anwendung, der dem Support von Structify dient, und, sofern eingesetzt, der Schutz der Anmeldeseite vor automatisierten Angriffen), beschreibt die Datenschutzerklärung; für Übermittlungen in Drittländer gilt dort Modul 2 der Standardvertragsklauseln.

Änderungen dieser Liste erfolgen nach § 5. Die aktuelle Fassung steht unter structify.solutions/rechtliches.