RECHTSTEXTE

Auftragsverarbeitungsvertrag

Anlage 1 zu den Allgemeinen Geschäftsbedingungen

Version 2.0 · gilt ab 08.10.2026

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 · gilt ab 08.10.2026

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 (im Browser, für macOS und Windows sowie für iOS und Android) 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), in Rechenzentren der Hetzner Online GmbH in Nürnberg und Falkenstein. 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 Auskunfts-, Berichtigungs-, Lösch- 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) **Zwei-Faktor-Authentifizierung.** Structify stellt für alle Nutzerkonten eine Zwei-Faktor-Authentifizierung bereit und empfiehlt ihre Einrichtung ausdrücklich (Anlage 2 Nr. 1). Ob die Nutzer des Verantwortlichen einen zweiten Faktor einrichten, liegt in der Verantwortung des Verantwortlichen und seiner Nutzer; der Verantwortliche berücksichtigt dies bei seiner eigenen Beurteilung der Angemessenheit der Sicherheitsmaßnahmen (Art. 32 DSGVO) und wirkt durch geeignete Anweisungen an seine Nutzer auf die Einrichtung hin. Beruht ein Schaden darauf, dass ein angebotener zweiter Faktor nicht eingerichtet war, ist er im Verhältnis der Parteien dem Verantwortlichen zuzurechnen, soweit nicht eine Verletzung der DSGVO oder dieses AVV durch Structify, etwa eine Sicherheitslücke der Plattform, den Schaden mitverursacht hat; in diesem Fall erfolgt die Aufteilung nach dem Maß der jeweiligen Verursachung (§ 11 Abs. 1, Art. 82 Abs. 4 und 5 DSGVO, § 254 BGB). Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

§ 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), in Rechenzentren der Hetzner Online GmbH: die Datenbank im Rechenzentrum Nürnberg, die Dateiablagen und 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 im Browser und für macOS und Windows

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, 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.

Die App für macOS und Windows greift auf dieselben Daten zu wie Structify im Browser; 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 für iOS und Android

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); Gerätekennung 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. Nach Ende des Hauptvertrags oder eines Test- und Demozugangs bleiben noch nicht übertragene Erfassungen bis zu 30 Tage auf dem Gerät (§ 25 Abs. 6 AGB). 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 (Rechenzentren Nürnberg und Falkenstein, § 8 Abs. 1). Daten aus der Vorgängerversion von Structify Operate liegen bis zu ihrer Löschung zusätzlich bei dem bisherigen Entwicklungs- und Hosting-Dienst Lovable Cloud (Anlage 3); übernommen werden sie nicht. 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 Hetzner Online GmbH in Nürnberg und Falkenstein (Anlage 3) mit physischer Zutrittskontrolle; Structify betreibt keine eigenen Serverräume.
- **Zugang zu den Servern:** Verwaltung der von Structify betriebenen Server ausschließlich per SSH-Schlüssel, kein Zugang mit Passwort; Datenbank und Verwaltungsoberflächen sind nicht öffentlich erreichbar (Zugriff nur intern bzw. über ein verschlüsseltes privates Netz für den Sicherungsserver); Firewall auf Anbieter- und Serverebene; automatische Sicherheitsaktualisierungen.
- **Zugang zu Nutzerkonten:** Anmeldung nur nach Authentifizierung; Schutz der Anmeldung und der Funktion „Passwort vergessen“ vor automatisierten Angriffen. Für alle Nutzerkonten steht eine Zwei-Faktor-Authentifizierung zur Verfügung (Einmalcodes nach TOTP oder Sicherheitsschlüssel und Passkeys nach dem WebAuthn-Standard). Die Einrichtung ist freiwillig und wird ausdrücklich empfohlen; Konten ohne zweiten Faktor erhalten einen Hinweis. Ein eingerichteter zweiter Faktor wird bei der Anmeldung verbindlich abgefragt. Über die Einrichtung entscheiden die Nutzer des Verantwortlichen; der Verantwortliche kann sie seinen Nutzern durch Anweisung vorgeben, eine technische Erzwingung je Organisation ist nicht vorgesehen (§ 4 Abs. 5). Für die Konten der Plattformadministration von Structify ist ein zweiter Faktor verpflichtend; ihre Anmeldungen werden serverseitig protokolliert. 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 auf Projektinhalte nur für Mitglieder des jeweiligen Projekts; 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 auf einem von Structify verwalteten Server im Rechenzentrum Nürnberg der Hetzner Online GmbH; Dateiablagen im Objektspeicher des Anbieters im Rechenzentrum Falkenstein mit Versionierung (überschriebene oder gelöschte Dateien sind 30 Tage wiederherstellbar).
- Fortlaufende Sicherung der Datenbank: Archivierung jeder Änderung und tägliche Vollsicherung, jeweils vor der Ablage verschlüsselt, auf getrenntem Speicher im Rechenzentrum Falkenstein; Vorhaltung sieben tägliche und vier wöchentliche Stände.
- Zusätzlich stündliche Sicherung der Datenbank auf einem von Structify verwalteten Sicherungsserver mit getrenntem Speicherplatz (Storage Box) im Rechenzentrum Falkenstein; Vorhaltung gestuft: stündliche Stände 48 Stunden, tägliche 35 Tage, wöchentliche 12 Wochen, monatliche 6 Monate. Dateiablagen werden stündlich gespiegelt; gelöschte oder überschriebene Dateien bleiben dort 90 Tage erhalten.
- Die Sicherungskopien werden vor der Ablage verschlüsselt (Datenbank: BorgBackup mit AES; Dateiablagen: rclone crypt mit AES einschließlich Datei- und Ordnernamen). Auf dem Sicherungsspeicher liegen nur verschlüsselte Daten; die Schlüssel verbleiben bei Structify. Zusätzlich tägliche Momentaufnahmen des Sicherungsspeichers.
- Tägliche Abbilder der Server durch den Hosting-Anbieter (sieben Stände, beim Anbieter in Deutschland, nicht von Structify verschlüsselt). Der verschlüsselte Datenträger der Datenbank (Nr. 4) geht nicht in diese Abbilder ein; sie können aber Reste der Datenbank aus gelöschten Dateien auf dem Systemdatenträger enthalten. Die Abbilder werden nach sieben Tagen automatisch gelöscht.
- Wiederhergestellt wird auf einen vorhandenen Sicherungsstand. Eine minutengenaue Wiederherstellung auf einen beliebigen Zeitpunkt wird nicht zugesagt.
- Wöchentliche automatische Prüfung der Sicherungen auf Vollständigkeit und Lesbarkeit; automatische Alarmierung der Geschäftsführung bei ausbleibenden oder fehlgeschlagenen Läufen.
- Wiederherstellungsübungen vierteljährlich; Übungen am 26. und 27.09.2026 mit vollständiger Wiederherstellung der Datenbank und der Dateiablagen in eine isolierte Umgebung sowie am 05.10.2026 mit einer Wiederherstellung der fortlaufenden Datenbanksicherung in eine isolierte Umgebung (alle Prüfwerte identisch).
- **Wiederherstellungszeiten (zugesichert, ab Kenntnis des Verlusts):** Teilverlust (einzelne Datensätze, Tabellen, Dateien) höchstens 2 Stunden; Totalverlust der Datenbank 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, Zeiten, in denen der Infrastruktur-Anbieter selbst großflächig nicht verfügbar ist, sowie der Verlust des Zugangs zum Konto beim Infrastruktur-Anbieter (etwa durch Sperrung oder Kündigung durch den Anbieter); da die Sicherungskopien derzeit beim selben Anbieter liegen, gilt hierfür keine zugesicherte Wiederherstellungszeit.

- Löschungen wirken in Sicherungskopien mit deren Auslaufen (spätestens sechs Monate); bei einer Wiederherstellung werden zuvor gelöschte Daten nicht reaktiviert.
- **Abschlusssicherung des bisherigen Datenbankdienstes:** Den Stand der Umstellung vom 06.10.2026 hat Structify vor der Löschung beim bisherigen Anbieter verschlüsselt im Objektspeicher im Rechenzentrum Falkenstein abgelegt, ausschließlich zum Nachweis der vollständigen Übernahme. Die Datenbankteile werden spätestens am 06.04.2027, die Dateien spätestens am 04.01.2027 gelöscht.

4. Verschlüsselung

- Transportverschlüsselung (TLS) für die Datenübertragung über öffentliche Netze; der Sicherungsserver ist über ein verschlüsseltes privates Netz angebunden.
- Verschlüsselung aller von Structify erstellten Sicherungskopien vor der Ablage; die Schlüssel verbleiben bei Structify.
- Zusätzliche Verschlüsselung besonders schutzbedürftiger gespeicherter Geheimnisse, etwa Zugangsschlüssel zu angebundenen Diensten.
- Verschlüsselung des Datenträgers, auf dem die Datenbank liegt (vollständige Datenträgerverschlüsselung mit LUKS2, AES-256 im XTS-Modus), seit dem 07.10.2026. Damit der Datenbankserver ohne manuellen Eingriff starten kann, liegt der Schlüssel zugriffsgeschützt auf dem Systemdatenträger dieses Servers und ist damit auch in dessen täglichen Abbildern (Nr. 3) enthalten; die Verschlüsselung schützt die Datenbank daher vor allem bei einem Zugriff auf den Datenträger außerhalb des laufenden Servers, nicht bei einem Zugriff, der zugleich diese Abbilder umfasst.
- Nicht zusätzlich verschlüsselt sind die Systemdatenträger der Server (Betriebssystem, Programme und Protokolldaten) und der Objektspeicher für die Dateiablagen; sie befinden sich in zutrittsgeschützten Rechenzentren in Deutschland (Nr. 1).

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 Liste: 08.10.2026. 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
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting der Plattform: Server, auf denen Structify Datenbank, Anmeldung, Server-Funktionen und Echtzeitdienst selbst betreibt und die Anwendungen ausliefert; Objektspeicher für die Dateiablagen; Datensicherung (Sicherungsserver und getrennter Speicher für ausschließlich verschlüsselte Sicherungskopien); Webhosting für die E-Mail-Postfächer von Structify, etwa für Support per E-Mail	Nürnberg und Falkenstein, Deutschland	kein Drittland
Anthropic PBC, USA (Vertragspartner im EWR: Anthropic Ireland, Limited)	KI-Auswertung von Text, Bildern und Dokumenten, Assistent „KAI“, Vorschläge, Volltexterfassung von Dokumenten für die Suche; 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

Nur bei Nutzung der jeweiligen Funktion

Unterauftragsverarbeiter	Leistung	Datenstandort	Drittland und Grundlage
Oneflow AB, Stockholm, Schweden	elektronische Signatur von Dokumenten einschließlich der Daten der Unterzeichnenden	EU (Irland, Sicherung Schweden)	kein Drittland

Frühere Unterauftragsverarbeiter

Die folgenden Anbieter setzt Structify nicht mehr ein. Sie sind aufgeführt, solange dort noch Daten liegen können oder die Beendigung kürzlich erfolgt ist.

Anbieter	bisherige Leistung	Stand
Supabase Pte. Ltd., Singapur	Datenbank, Anmeldung, Dateispeicher und Server-Funktionen (Datenstandort Frankfurt am Main) bis zur Umstellung auf Hetzner am 06.10.2026	Projekte am 07.10.2026 gelöscht. Die Abschlusssicherung liegt verschlüsselt ausschließlich bei Hetzner in Falkenstein (Anlage 2 Nr. 3).

Anbieter	bisherige Leistung	Stand
Vercel Inc., USA	Auslieferung der Webanwendung bis 07.10.2026	Projekte am 07.10.2026 gelöscht; keine Verarbeitung mehr.
RunPod, Inc., USA	Rechenleistung für begehbare 3D-Rundgänge aus Begehungsvideos	Funktion stillgelegt; Structify übermittelt keine Daten mehr an RunPod. Etwa dort noch vorhandene Daten früherer Verarbeitungen werden gelöscht.
IONOS SE, Montabaur, Deutschland	E-Mail-Postfächer von Structify, etwa für Support per E-Mail, bis zum Umzug zu Hetzner am 06.10.2026	Postfächer am 08.10.2026 gelöscht; kein laufender Betrieb. E-Mails aus der Zeit bis zum 06.10.2026 bewahrt Structify im revisionssicheren E-Mail-Archiv der IONOS SE nur noch zur Erfüllung eigener gesetzlicher Aufbewahrungspflichten auf (§ 257 HGB, § 147 AO; § 10 Abs. 4); insoweit ist Structify selbst Verantwortlicher und IONOS kein Unterauftragsverarbeiter. Löschung nach Ablauf der Aufbewahrungsfrist (Datenschutzerklärung G8); kein Drittland.
Lovable Cloud	Hosting der Vorgängerversion von Structify Operate	Daten aus der Vorgängerversion liegen dort bis zu ihrer Löschung; sie werden weder übernommen noch weiter genutzt.

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, die Terminbuchung für Gespräche mit Structify (Cal.com) und der Schutz der Anmeldeseiten vor automatisierten Angriffen (Cloudflare Turnstile), 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.