

Auftragsverarbeitungsvertrag (AVV)

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten durch Bornwerk im Auftrag des Geschäftskunden nach Art. 28 DSGVO. Sie wird mit Vertragsschluss Bestandteil des Vertrags.

Stand: 25. Oktober 2026

Worum es geht

Wenn Sie Terminz für Ihren Betrieb nutzen, verarbeitet Bornwerk personenbezogene Daten Ihrer Kunden und Mitarbeiter in Ihrem Auftrag. Sie bleiben dabei Verantwortlicher, Bornwerk ist Auftragsverarbeiter. Art. 28 DSGVO verlangt dafür einen Vertrag, der die Pflichten des Auftragsverarbeiters festlegt.

Diese Seite ist dieser Vertrag. Sie müssen ihn nicht anfordern und nicht gesondert unterzeichnen: Er ist Anlage zu Teil B der Allgemeinen Geschäftsbedingungen und kommt nach Art. 28 Abs. 9 DSGVO in elektronischer Form mit dem Vertrag zustande. Für die Verarbeitungen, bei denen Bornwerk selbst Verantwortlicher ist, gilt stattdessen die Datenschutzerklärung.

Vertragsparteien

AUFTRAGSVERARBEITER

Bo

Bornwerk UG (haftungsbeschränkt)

Märkische Straße 193, 44141 Dortmund, Deutschland
datenschutz@terminz.com

VERANTWORTLICHER

Der Rechtsträger, der Vertragspartner des jeweiligen Terminz-Vertrags ist und Terminz zur Verarbeitung von Kundendaten nutzt. Je Rechtsträger besteht ein eigener Vertrag und ein eigener AVV; mehrere Standorte desselben Rechtsträgers sind von derselben Vereinbarung erfasst.

§ 1 Gegenstand und Rangfolge

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien, die sich aus der Nutzung der Software nach Teil B der Allgemeinen Geschäftsbedingungen ergeben. Sie gilt für alle Verarbeitungen personenbezogener Daten, die Bornwerk für den Geschäftskunden durchführt.

Bei Widersprüchen zwischen dieser Vereinbarung und den übrigen Bestimmungen des Vertrags gehen die Regelungen dieser Vereinbarung vor, soweit die Verarbeitung personenbezogener Daten betroffen ist.

§ 2 Rollen der Parteien

Der Geschäftskunde ist Verantwortlicher nach Art. 4 Nr. 7 DSGVO für die personenbezogenen Daten seiner Endkunden und seiner Mitarbeiter, die er über die Software verarbeitet. Er allein hat sicherzustellen, dass für diese Verarbeitung eine Rechtsgrundlage besteht und dass die betroffenen Personen nach Art. 13 und 14 DSGVO informiert werden.

Bornwerk ist insoweit Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO. Für die eigenen Verarbeitungen von Bornwerk — insbesondere die Vertrags-, Abrechnungs- und Kontodaten des Geschäftskunden sowie die Besucherdaten auf terminz.com — ist Bornwerk Verantwortlicher; hierfür gilt die Datenschutzerklärung und nicht diese Vereinbarung.

Je Rechtsträger besteht ein eigener Vertrag und damit eine eigene Vereinbarung zur Auftragsverarbeitung. Betreibt der Geschäftskunde mehrere Standorte unter demselben Rechtsträger, sind diese von derselben Vereinbarung erfasst.

Legt ein Endnutzer bei Bornwerk ein eigenes Nutzerkonto an, ist Bornwerk für die von diesem Endnutzer selbst angegebenen Konto- und Anmeldedaten sowie für dessen betriebsübergreifende Terminübersicht Verantwortlicher; Rechtsgrundlage ist der Nutzungsvertrag nach Teil A der Allgemeinen Geschäftsbedingungen (Art. 6 Abs. 1 lit. b DSGVO). Ebenso ist Bornwerk Verantwortlicher für das plattformweit geführte Profil der Kontaktdaten einer Person. Aus diesem Profil erhält der Geschäftskunde nur die Angaben, die die Person ihm freigegeben hat; vor der Freigabe erhält er den verkürzten Namen und den Status der Freigabe. Eine bereits vorhandene Person kann er nur über ihre vollständige E-Mail-Adresse oder Telefonnummer auffinden, und nur, wenn sie auffindbar ist. Diese Verarbeitungen sind nicht Gegenstand dieser Vereinbarung.

Mit der Freigabe gelangen die freigegebenen Angaben in die Kundenakte des Geschäftskunden; ab diesem Zeitpunkt ist er für sie Verantwortlicher und Bornwerk Auftragsverarbeiter. Das Gleiche gilt für die Angaben, die der Geschäftskunde selbst über einen Endnutzer erhebt oder ergänzt, insbesondere für die von ihm erfassten Kontaktangaben („Eigene Angaben“). Sie werden anderen Geschäftskunden nicht zugänglich gemacht. Eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO besteht nicht.

§ 3 Dauer

Diese Vereinbarung kommt mit dem Vertrag nach B.3 der Allgemeinen Geschäftsbedingungen zustande und läuft für dessen Dauer. Sie endet mit der Beendigung des Vertrags, ohne dass es einer gesonderten Kündigung bedarf.

Eine Kündigung dieser Vereinbarung ohne gleichzeitige Beendigung des Vertrags ist ausgeschlossen. Die Pflichten aus § 12 bestehen über das Ende dieser Vereinbarung hinaus fort.

§ 4 Gegenstand, Art und Zweck der Verarbeitung

Bornwerk verarbeitet personenbezogene Daten ausschließlich zum Zweck der Bereitstellung und des Betriebs der vertraglich vereinbarten Software: Terminbuchung und Terminverwaltung, Kunden- und Personalverwaltung, Zeiterfassung, Zahlungs- und Kassenfunktion, Benachrichtigungen sowie die öffentliche Profilseite des Geschäftskunden. Dazu gehört auf Weisung des Geschäftskunden die Übernahme von Leistungen, Mitarbeitern und Terminen aus einem Export seines bisherigen Systems.

Die Verarbeitung umfasst das Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln, Einschränken, Löschen und Vernichten personenbezogener Daten. Sie findet in Mitgliedstaaten der Europäischen Union statt, soweit § 14 nichts anderes bestimmt.

§ 5 Kategorien betroffener Personen und Daten

Betroffen sind die Endkunden des Geschäftskunden, seine Mitarbeiter und Mitwirkenden sowie die Ansprechpartner seiner Geschäftspartner. Verarbeitet werden folgende Datenkategorien:

- Stammdaten: Anrede, Vor- und Nachname, Geburtsdatum
- Kontaktdaten: E-Mail-Adresse, Telefonnummer, Anschrift
- Termin- und Vertragsdaten: gebuchte Leistungen, Termin- und Besuchshistorie, Zuordnung zu Mitarbeitern, Stornierungen und Nichterscheinen
- Zahlungs- und Kassendaten: Beleg- und Rechnungsdaten, Zahlungsart, Betrag, Transaktionskennungen, Gutscheine und Guthaben
- Nutzungsdaten: Kontokennungen, Anmeldezeitpunkte, Protokolldaten der Anwendung
- Beschäftigtendaten: Arbeits- und Abwesenheitszeiten, Qualifikationen und vergütungsrelevante Angaben, soweit der Geschäftskunde die Personalfunktionen nutzt
- Freitextangaben: Notizen des Geschäftskunden zu Kunden und Terminen
- Bilddaten: Fotos und Vorher-Nachher-Bilder, die der Geschäftskunde auf seiner Buchungsseite veröffentlicht, einschließlich darauf erkennbarer Personen
- Besondere Kategorien nach Art. 9 DSGVO: Gesundheitsangaben, soweit der Geschäftskunde branchenspezifische Felder oder Freitextnotizen dafür nutzt

Für die Verarbeitung besonderer Kategorien personenbezogener Daten ist allein der Geschäftskunde verantwortlich. Er hat sicherzustellen, dass ein Erlaubnistatbestand nach Art. 9 Abs. 2 DSGVO vorliegt – im Regelfall die ausdrückliche Einwilligung der betroffenen Person nach Art. 9 Abs. 2 lit. a DSGVO – und dass solche Angaben nicht in Feldern erfasst werden, die dafür nicht vorgesehen sind. Die Einwilligung der auf Bilddaten erkennbaren Personen holt der Geschäftskunde selbst ein und weist sie nach (Art. 6 Abs. 1 lit. a, Art. 7 Abs. 1 DSGVO); die Software lässt die Veröffentlichung eines solchen Fotos erst zu, nachdem der Geschäftskunde dies bestätigt hat.

§ 6 Weisungsrecht

Bornwerk verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Geschäftskunden, einschließlich einer Übermittlung in Drittländer (Art. 28 Abs. 3 lit. a DSGVO). Der Vertrag samt dieser Vereinbarung sowie die Einstellungen, die der Geschäftskunde in der Software vornimmt, sind die Erstweisung.

Einzelweisungen erteilt der Geschäftskunde in Textform an datenschutz@terminz.com. Weisungsbefugt sind der Inhaber des Rechtsträgers und die von ihm benannten Personen.

Ist Bornwerk der Auffassung, dass eine Weisung gegen die Datenschutz-Grundverordnung oder andere Datenschutzbestimmungen verstößt, teilt Bornwerk dies dem Geschäftskunden unverzüglich mit (Art. 28 Abs. 3 UAbs. 2 Satz 2 DSGVO) und darf die Durchführung bis zu ihrer Bestätigung oder Änderung aussetzen.

Mit Abschluss des Vertrags weist der Geschäftskunde Bornwerk an, (a) eine Verknüpfung einer Person mit seinem Betrieb zu lösen, wenn die Person sie ablehnt („Das war ich nicht“), und ihm die dabei anfallenden Branchenangaben in einer Übergabedatei bereitzustellen, (b) die Kundenakte einer Person, die ihr Nutzerkonto löscht, nach § 12 Abs. 6 zu sperren und nach Fristablauf zu löschen, und (c) Anträge betroffener Personen, die die Kundenakte betreffen, an ihn weiterzuleiten (§ 10 Abs. 2).

§ 7 Vertraulichkeit

Bornwerk setzt für die Verarbeitung ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung besteht nach Beendigung der Tätigkeit fort.

Die eingesetzten Personen werden vor Aufnahme der Tätigkeit mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht.

§ 8 Technische und organisatorische Maßnahmen

Bornwerk trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau sicherzustellen (Art. 28 Abs. 3 lit. c DSGVO). Die getroffenen Maßnahmen sind in Anlage 2 beschrieben.

Bornwerk darf die Maßnahmen an den Stand der Technik anpassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden in Anlage 2 nachgeführt.

Bornwerk unterhält für Support und Fehlerbehebung einen administrativen Zugang zu den im Auftrag verarbeiteten Daten. Er ist auf wenige benannte, nach § 7 zur Vertraulichkeit verpflichtete Personen beschränkt und wird nur zur Vertragserfüllung oder auf Weisung des Geschäftskunden genutzt.

§ 9 Unterauftragsverarbeiter

Der Geschäftskunde erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen (Art. 28 Abs. 2 Satz 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 1 aufgeführt und damit genehmigt.

Bornwerk informiert den Geschäftskunden mindestens 30 Tage vor der Hinzuziehung eines neuen oder dem Wechsel eines bestehenden Unterauftragsverarbeiters in Textform an die im Konto hinterlegte E-Mail-Adresse. Der Geschäftskunde kann der Änderung innerhalb von 14 Tagen nach Zugang aus einem datenschutzrechtlichen Grund widersprechen.

Widerspricht der Geschäftskunde, suchen die Parteien eine einvernehmliche Lösung. Kann Bornwerk die Leistung ohne den betroffenen Unterauftragsverarbeiter nicht in zumutbarer Weise erbringen, kann der Geschäftskunde den Vertrag zum Wirksamwerden der Änderung außerordentlich kündigen.

Bornwerk erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO), und haftet für dessen Verhalten wie für eigenes.

Reine Hilfsleistungen wie Telekommunikations-, Reinigungs- oder Wartungsleistungen sind keine Unterauftragsverarbeitung im Sinne dieser Vereinbarung.

§ 10 Unterstützung des Verantwortlichen

Bornwerk unterstützt den Geschäftskunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Art. 12 bis 23 DSGVO zu beantworten (Art. 28 Abs. 3 lit. e DSGVO). Was der Geschäftskunde nicht selbst in der Software erledigen kann, insbesondere die Herausgabe der Daten einer Person in maschinenlesbarer Form, setzt Bornwerk auf seine Weisung in Textform um.

Wendet sich eine betroffene Person unmittelbar an Bornwerk, leitet Bornwerk den Antrag unverzüglich an den Geschäftskunden weiter und beantwortet ihn nicht selbst, soweit er die Verarbeitung im Auftrag betrifft.

Bornwerk unterstützt den Geschäftskunden ferner bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung und einer vorherigen Konsultation der Aufsichtsbehörde, unter Berücksichtigung der Art der Verarbeitung und der Bornwerk zur Verfügung stehenden Informationen (Art. 28 Abs. 3 lit. f DSGVO).

§ 11 Verletzungen des Schutzes personenbezogener Daten

Bornwerk meldet dem Geschäftskunden jede Verletzung des Schutzes personenbezogener Daten, die die im Auftrag verarbeiteten Daten betrifft, unverzüglich nach Bekanntwerden in Textform an die im Konto hinterlegte E-Mail-Adresse (Art. 33 Abs. 2 DSGVO).

Die Meldung beschreibt, soweit verfügbar, die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen und vorgeschlagenen Maßnahmen. Noch fehlende Angaben werden unverzüglich nachgereicht.

Die Meldung an die Aufsichtsbehörde nach Art. 33 Abs. 1 DSGVO und die Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO obliegen dem Geschäftskunden; Bornwerk unterstützt ihn dabei.

§ 12 Löschung und Rückgabe

Nach Beendigung des Vertrags löscht Bornwerk alle im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie zurück, nach Wahl des Geschäftskunden (Art. 28 Abs. 3 lit. g DSGVO); für die Archivkopie gilt Absatz 3. Der Geschäftskunde teilt seine Wahl bis zum Vertragsende mit; trifft er keine Wahl, werden die Daten gelöscht.

Der Geschäftskunde erhält seine Daten nach B.18 der Allgemeinen Geschäftsbedingungen: Kassen- und Buchhaltungsdaten während der Vertragslaufzeit und nach Vertragsende bis zur Löschung selbst über die Exporte der Software, alle übrigen auf Anforderung als Excel-Datei (XLSX), jeweils in einem strukturierten, gängigen und maschinenlesbaren Format. Nach Vertragsende hält Bornwerk die Daten noch 90 Tage bereit, stellt die übrigen Daten in dieser Zeit weiter auf Anforderung bereit und erinnert vor der Löschung per E-Mail daran.

Löscht der Geschäftskunde ein veröffentlichtes Foto, entfernt Bornwerk die Bilddatei einschließlich aller Vorschaugrößen aus dem Speicher und veranlasst, dass zwischengespeicherte Kopien im Auslieferungsnetz gelöscht werden.

Die Aufbewahrung von Kassen-, Beleg- und Rechnungsdaten nach § 147 AO, § 257 HGB und der Kassensicherungsverordnung obliegt dem Geschäftskunden. Er exportiert diese Daten vor dem Ende des Abrufzeitraums; danach werden sie mit den übrigen Daten gelöscht. Unabhängig davon weist der Geschäftskunde Bornwerk an, die Archivkopie nach B.18 der Allgemeinen Geschäftsbedingungen über das Vertragsende hinaus bis zum Ablauf der dort genannten Frist in einem gegen Änderung gesperrten Speicher in der Europäischen Union aufzubewahren und danach zu löschen (Art. 28 Abs. 3 lit. a und g DSGVO). Bornwerk verarbeitet die Archivkopie nur, um sie aufzubewahren und dem Geschäftskunden bereitzustellen; verlangt er nach Vertragsende ihre Herausgabe und Löschung, verfährt Bornwerk nach B.18. Für die Dauer der Aufbewahrung gilt diese Vereinbarung fort.

Abrechnungsbelege behalten die bei Ausstellung erfassten Angaben des Empfängers. Ein Löschverlangen nach Art. 17 DSGVO erfasst sie nicht, solange die Aufbewahrungspflicht besteht (Art. 17 Abs. 3 lit. b DSGVO).

Sicherungskopien werden im Rahmen der regulären Rotation überschrieben; eine gezielte Löschung einzelner Datensätze aus bestehenden Sicherungskopien erfolgt nicht.

Löscht eine Person ihr Nutzerkonto, sperrt Bornwerk die Kundenakte des Geschäftskunden zu dieser Person: Notizen, Branchen- und Gesundheitsprofile bleiben bis zum 31. Dezember des dritten Jahres nach dem Jahr des letzten Termins, Besuchs oder Belegs bei diesem Betrieb gesperrt, bei einem Betrieb der Gesundheitsbranche des zehnten Jahres. Die Namen auf den einzelnen Terminen werden je Termin zum 31. Dezember des dritten Jahres nach dem Jahr des Termins anonymisiert, bei der Gesundheitsbranche des zehnten Jahres. Gesperrte Daten liest nur der Inhaber des Betriebs und nur zur Abwehr von Ansprüchen oder zur Erfüllung einer Dokumentationspflicht (Einschränkung der Verarbeitung nach Art. 18 DSGVO). Bornwerk informiert den Geschäftskunden per E-Mail und im Dashboard und löscht die Akte nach Fristablauf; der Geschäftskunde kann sie vorher löschen.

§ 13 Nachweise und Überprüfungen

Bornwerk stellt dem Geschäftskunden alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind (Art. 28 Abs. 3 lit. h DSGVO). Der Nachweis kann durch aktuelle Selbstauskünfte, die Dokumentation nach Anlage 2 oder durch Prüfberichte und Zertifikate unabhängiger Stellen geführt werden.

Reichen diese Nachweise im Einzelfall nicht aus, ermöglicht Bornwerk dem Geschäftskunden oder einem von ihm beauftragten, zur Verschwiegenheit verpflichteten und nicht mit Bornwerk im Wettbewerb stehenden Prüfer eine Überprüfung. Sie erfolgt nach Ankündigung mit einer Frist von 30 Tagen, während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und höchstens einmal je Kalenderjahr; aus besonderem Anlass, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten oder auf Anordnung einer Aufsichtsbehörde, auch häufiger.

Der Geschäftskunde trägt die Kosten einer von ihm veranlassten Überprüfung. Für den eigenen Aufwand kann Bornwerk eine angemessene Vergütung verlangen, es sei denn, die Überprüfung ergibt einen von Bornwerk zu vertretenden Verstoß.

§ 14 Übermittlung in Drittländer

Die Verarbeitung findet grundsätzlich in Deutschland statt. Soweit einzelne Unterauftragsverarbeiter Daten außerhalb der Europäischen Union verarbeiten, ist dies in Anlage 1 ausgewiesen.

Eine Übermittlung erfolgt nur, wenn die Voraussetzungen des Kapitels V DSGVO erfüllt sind: auf Grundlage eines Angemessenheitsbeschlusses nach Art. 45 DSGVO, insbesondere des EU-US Data Privacy Framework, oder auf Grundlage der Standardvertragsklauseln der Europäischen Kommission nach Art. 46 Abs. 2 lit. c DSGVO nebst ergänzenden Maßnahmen.

§ 15 Haftung und Schlussbestimmungen

Für die Haftung gilt B.17 der Allgemeinen Geschäftsbedingungen. Art. 82 DSGVO bleibt unberührt.

Bornwerk ist nicht verpflichtet, einen Datenschutzbeauftragten zu benennen; die Voraussetzungen des Art. 37 DSGVO und des § 38 BDSG liegen nicht vor. Ansprechpartner in Datenschutzfragen ist die unten genannte Kontaktadresse.

Bornwerk kann diese Vereinbarung ändern, soweit dies durch eine Änderung der Rechtslage, durch Vorgaben einer Aufsichtsbehörde oder durch Rechtsprechung veranlasst ist. Die Änderung wird mindestens 30 Tage vor Wirksamwerden in Textform mitgeteilt; widerspricht der Geschäftskunde nicht innerhalb dieser Frist, gilt sie

als angenommen. Auf das Widerspruchsrecht und die Folgen des Schweigens wird in der Mitteilung hingewiesen.

Änderungen im Übrigen bedürfen der Textform. Ist eine Bestimmung unwirksam, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 – Unterauftragsverarbeiter

Die folgenden Unterauftragsverarbeiter sind nach § 9 dieser Vereinbarung genehmigt. Alle unterliegen einem Vertrag nach Art. 28 DSGVO; bei Verarbeitung außerhalb der EU sind die Garantien nach Kapitel V DSGVO ausgewiesen.

Anbieter	Zweck	Standort	Schutzmaßnahme
Hetzner Online GmbH	Betrieb der Anwendungsserver und der Datenbank; außerdem Weiterleitung der Hauptdomain eigener Domains auf www	Deutschland (Falkenstein)	Verarbeitung ausschließlich in Deutschland
Amazon Web Services EMEA SARL	Objektspeicher für hochgeladene Dateien, Verwaltung von Zugangsdaten und verschlüsselte Datenbanksicherungen	Deutschland (Region eu-central-1, Frankfurt)	Speicherung ausschließlich in Deutschland; Standardvertragsklauseln für Support-Zugriffe des Mutterkonzerns
Cloudflare Germany GmbH / Cloudflare, Inc.	Content Delivery Network, Reverse-Proxy und Auslieferung der Medien; verarbeitet jede eingehende Anfrage einschließlich IP-Adresse; außerdem TLS-Terminierung und Auslieferung der Website über eigene Domains der Geschäftskunden	EU-Edge / weltweit	EU-US Data Privacy Framework, ergänzend Standardvertragsklauseln
Stripe Payments Europe, Ltd. / Stripe, Inc.	Zahlungsabwicklung einschließlich Kartenzahlungen am Kartenlesegerät	Irland / USA	EU-US Data Privacy Framework, ergänzend Standardvertragsklauseln
fiskaly GmbH	Signatur der Kassentransaktionen durch die zertifizierte technische Sicherheitseinrichtung nach der Kassensicherungsverordnung; übermittelt werden Beträge, Steuersätze, Zahlungsart und die Kennung der Kasse, nicht Namen oder Kontaktdaten der Endkunden	Österreich (Wien)	Verarbeitung in der EU

Anbieter	Zweck	Standort	Schutzmaßnahme
Resend (Plus Five Five, Inc.)	Versand der Transaktions-E-Mails an Endkunden und Mitarbeiter, etwa Buchungsbestätigung, Erinnerung und Beleg	USA	EU-US Data Privacy Framework, ergänzend Standardvertragsklauseln
Functional Software, Inc. (Sentry)	Erkennung technischer Fehler der Anwendung; übermittelt werden Vorgangsname, Fehlercode, aufgerufene Seite, Namen und Fehlercodes der vorausgehenden Vorgänge, die Form (Feldname, Typ, Länge) gesendeter Felder und ein monatlich wechselndes Standort- Pseudonym, nicht die Inhalte der Anwendung	EU-Region (Frankfurt)	Speicherung in der EU; Support-Zugriff aus den USA auf Grundlage des EU-US Data Privacy Framework bzw. der Standardvertragsklauseln
Google Ireland Ltd. / Google LLC	Google Maps Plattform: Adressvervollständigung bei der Eingabe einer Anschrift sowie Kartendarstellung auf der öffentlichen Profilseite	Irland / USA	EU-US Data Privacy Framework, ergänzend Standardvertragsklauseln
Google Ireland Ltd. / Google LLC	Google Identity Services: Anmeldung mit einem Google-Konto im Buchungsvorgang und im Kundenkonto	Irland / USA	EU-US Data Privacy Framework, ergänzend Standardvertragsklauseln

Reichweitenmessung und Analyse auf terminz.com sind nicht Gegenstand dieser Vereinbarung: Dort ist Bornwerk selbst Verantwortlicher. Diese Dienste laufen nicht auf den Buchungs- und Profilseiten Ihres Betriebs.

Anlage 2 — Technische und organisatorische Maßnahmen

Maßnahmen nach Art. 32 DSGVO im Zeitpunkt des Stands dieser Vereinbarung.

VERTRAULICHKEIT UND ZUGRIFFSKONTROLLE

- Zugang zur Anwendung nur nach Anmeldung. Fünf Rollenstufen vom Endkunden bis zur Systemverwaltung; jede geschäftsbezogene Abfrage prüft zusätzlich, ob der Aufrufende dem betreffenden Rechtsträger angehört.
- Die Mandantentrennung ist automatisiert abgesichert: Fehlt für eine Listenabfrage der Test auf mandantenfremden Zugriff, schlägt die Auslieferung fehl.
- Zwei-Faktor-Authentisierung über Einmalkennwort und Passkeys steht allen Konten zur Verfügung und wird bei erhöhtem Anmeldeisiko verlangt. Anmeldeversuche werden stufenweise gesperrt.
- Passwörter werden mit Argon2 gespeichert, Kassen-PINs mit bcrypt, Sitzungstoken zur Verlängerung als Hashwert. Bankverbindungen werden verschlüsselt abgelegt; ohne gültigen Schlüssel startet die Anwendung im Produktivbetrieb nicht.
- Für Support und Fehlerbehebung besteht ein administrativer Zugang von Bornwerk zu den Daten des Geschäftskunden. Er ist auf wenige benannte, nach § 7 zur Vertraulichkeit verpflichtete Personen

beschränkt und wird nur zur Vertragserfüllung oder auf Weisung genutzt.

INTEGRITÄT

- Übertragung ausschließlich über TLS 1.2 und 1.3, mit erzwungener Weiterleitung auf HTTPS und HSTS über ein Jahr einschließlich Subdomains.
- Der Objektspeicher ist serverseitig verschlüsselt, öffentlich nicht erreichbar und weist unverschlüsselte Verbindungen ab.
- Hochgeladene Dateien werden vor der Ablage auf Schadsoftware geprüft; schlägt die Prüfung fehl oder ist der Prüfdienst nicht erreichbar, wird die Datei abgewiesen. Der Dateityp wird am Inhalt bestimmt, nicht an der Angabe des Browsers; Vektorgrafiken werden bereinigt.
- Sicherheitsrelevante Ereignisse — Anmeldung, Rollen- und Rechteänderungen, Datenexporte, Notfallzugriffe — werden protokolliert.

VERFÜGBARKEIT UND BELASTBARKEIT

- Tägliche Sicherung der Datenbank, mit AES-256 verschlüsselt, mit Prüfsumme abgelegt und in der Größe verifiziert. Eine ausgebliebene Sicherung löst über eine Totmannschaltung einen Alarm aus.
- Die Wiederherstellung wurde zuletzt am 22. Juli 2026 vollständig geprüft: Die Sicherung wurde in eine getrennte Umgebung eingespielt, alle Tabellen und Datensatzzahlen stimmten mit dem Produktivsystem überein.
- Der Ursprungsserver nimmt Anfragen nur aus den Adressbereichen des vorgelagerten Netzwerkdienstes an; andere Anfragen werden verworfen.
- Ratenbegrenzung auf Netz- und Anwendungsebene sowie eine Verfügbarkeitsüberwachung, die von außerhalb des Produktivsystems prüft.

TRENNBARKEIT UND AUFTRAGSKONTROLLE

- Die Daten verschiedener Rechtsträger liegen in getrennten Datenräumen derselben Datenbank und werden über die Zugriffsprüfung getrennt gehalten.
- Entwicklung, Test und Produktivbetrieb sind getrennte Umgebungen mit eigenen Zugangsdaten und eigenen Speicherorten. Echtdaten werden nicht in Test- oder Entwicklungsumgebungen übernommen.
- Unterauftragsverarbeiter werden vor dem Einsatz geprüft und nach Art. 28 DSGVO vertraglich gebunden; die Liste ist in Anlage 1 veröffentlicht.

ÜBERPRÜFUNG UND BEWERTUNG

- Vor jeder Auslieferung wird der Quellcode automatisiert auf offengelegte Zugangsdaten und auf Sicherheitsmängel geprüft; Funde hoher Schwere brechen die Auslieferung ab. Container-Abbilder sind auf einen festen Prüfwert gebunden.
- Die Löschfristen laufen als geplanter täglicher Vorgang: Kennungen in Zugriffsprotokollen werden nach 30 Tagen entfernt, in Sitzungsdaten nach 90 Tagen, Anmeldeversuche nach 30 Tagen gelöscht.
- Die Maßnahmen dieser Anlage werden bei wesentlichen Änderungen fortgeschrieben; der Stand ergibt sich aus dem Datum dieser Vereinbarung.

Datenschutzkontakt

Weisungen nach § 6, Anfragen betroffener Personen und alle weiteren Fragen zu dieser Vereinbarung richten Sie bitte an:

✉ datenschutz@terminz.com

Zuständige Aufsichtsbehörde für Bornwerk ist die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Maßgeblich ist die deutsche Fassung dieser Vereinbarung.