# Vertrag über die Auftragsverarbeitung personenbezogener Daten

Zwischen dem

Kunden

als Auftraggeber
- nachfolgend Auftraggeber -

und

Planubo, Christoph Drechsler & Michael Tenzer GbR
Am Hirtengarten 2
77743 Neuried

als Auftragnehmer
- nachfolgend Auftragnehmer -

# 1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

# 2 Gegenstand und Dauer der Verarbeitung

## 2.1 Gegenstand

Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Erbringung von Leistungen nach dem Auftrag, der Leistungsbeschreibung und AGB (im Folgenden Hauptvertrag genannt), soweit eine Verarbeitung personenbezogener Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO stattfindet. Dazu gehören alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags durchführt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, wenn der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.
Nutzt der Auftraggeber eine kundeneigene Custom Domain oder einen eigenen SMTP-Server zur Kommunikation mit seinen Endkunden, ist und bleibt der Auftraggeber für die über diese Kanäle verarbeiteten personenbezogenen Daten alleiniger Verantwortlicher. Der Auftragnehmer verarbeitet in diesem Zusammenhang ausschließlich diejenigen personenbezogenen Daten, die auf seiner eigenen Infrastruktur verbleiben; für Daten, die über den vom Auftraggeber hinterlegten externen SMTP-Dienst versandt werden, ist der Auftragnehmer weder Verantwortlicher noch Auftragsverarbeiter.

## 2.2 Dauer

Die Verarbeitung beginnt an dem im Auftrag vereinbarten Startdatum und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

# 3 Art, Zweck und Betroffene der Datenverarbeitung:

## 3.1 Art und Zweck der Verarbeitung

Der Auftragnehmer erbringt für den Auftraggeber die Leistungen gemäß des Hauptvertrags. Darüber hinaus erbringt er Wartungs- und Supportleistungen für den Auftraggeber, wodurch die Möglichkeit des Zugriffs auf die nachstehend genannten Arten personenbezogener Daten besteht, die mit der Software verarbeitet oder auf dem zur Verfügung gestellten Speicherplatz gespeichert werden.

## 3.2 Art der Daten

Es werden folgende Daten verarbeitet:

- Die Art der verarbeiteten Daten wird vom Auftraggeber durch die Konfiguration und durch die Nutzung der Dienste bestimmt. Zu den zu verarbeitenden Daten können unter anderem Vor- und Nachname, E-Mail-Adresse, IP-Adresse, Adresse, Veranstaltungsdaten, Rechnungsdaten und Profileinstellungen gehören.
- Zu den zu verarbeitenden Daten können darüber hinaus folgende Daten gehören, sofern der Auftraggeber das SEPA-Modul nutzt:

- Bankverbindungsdaten der Endkunden des Auftraggebers (Kontoinhabername, IBAN, BIC),
- SEPA-Mandatsreferenzen, Mandatstexte und deren versionierter Snapshot,
- Beweissicherungsdaten zur Online-Mandatserteilung (IP-Adresse des Mandatsgebers, User-Agent, Zeitstempel, Sprache, angezeigter Mandatstext).

### 3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Die Kategorien von Betroffenen werden vom Auftraggeber durch die Konfiguration und durch die Nutzung der Dienste bestimmt. Zu den betroffenen Personen können Kunden des Auftraggebers, Interessenten des Auftraggebers, und Mitarbeiter des Auftraggebers gehören.

## 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung zuzuleiten. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Die Kontaktdaten des Datenschutzbeauftragten sind auf der Webseite des Auftragnehmers veröffentlicht.

## 5 Sicherheit der Verarbeitung

(1) Der Auftragnehmer trifft in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung in Übereinstimmung mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftraggeber ergreift in seinem Verantwortungsbereich angemessene technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung dauerhaft sicherzustellen.

(2) Die aktuellen technischen und organisatorischen Maßnahmen des Auftragnehmers können im Anhang 1 eingesehen werden. Dabei handelt es sich um Beschreibungen technischer Art handelt, die als Teil dieser Vereinbarung zu betrachten sind.

(3) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Schutzniveau nicht unterschritten wird.

## 6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Soweit eine betroffene Person sich bei Ausübung ihrer Datenschutzrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

## 7 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Subunternehmer im Sinne von Art. 28 DSGVO für die Erfüllung des Vertrags einzusetzen.

(2) Die derzeit verwendeten Subunternehmer sind in Anlage 2 aufgeführt. Der Auftraggeber gestattet den Einsatz dieser aufgeführten Subunternehmer. Die Auslagerung auf weitere Unterauftragnehmer sowie jeder Wechsel der gemäß Anlage 2 bestehenden Subunternehmer sind zulässig, soweit:
   a. der Auftragnehmer eine solche Auslagerung bzw. den Wechsel dem Auftraggeber mit einer Frist von 4 Wochen vorab schriftlich oder in Textform anzeigt und
   b. der Auftraggeber nicht innerhalb von 2 Wochen nach Erhalt der Anzeige gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt. Im Falle eines Einspruchs des Auftraggebers gegen eine solche Auslagerung bzw. gegen den Wechsel eines Subunternehmers hat der Auftragnehmer das Recht zur außerordentlichen Kündigung dieser Vereinbarung und des Hauptvertrags aus wichtigem Grund.

(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können.

(4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(5) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(6) Wenn der Auftragnehmer Aufträge an andere Auftragsverarbeiter vergibt, obliegt es dem Auftragnehmer, seine Datenschutzverpflichtungen aus dieser Vereinbarung auf den anderen Auftragsverarbeiter zu übertragen.

(7) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

## 8 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

(4) Im Falle einer Beendigung verpflichtet sich der Auftraggeber, die in den Diensten gespeicherten personenbezogenen Daten vor der Beendigung des Vertrags zu löschen.

(5) Auf Verlangen des Auftragnehmers benennt der Auftraggeber eine Kontaktperson für Datenschutzfragen.

## 9 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Berichtigungs-, Löschungs- oder Auskunftsersuchen an den Auftragnehmer, so verweist der Auftragnehmer die betroffene Person an den Auftraggeber, sofern eine Zuordnung zum Auftraggeber nach den Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet die Anfrage der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer wird den Auftraggeber im Rahmen seiner Möglichkeiten unterstützen. Der Auftragnehmer haftet nicht, wenn die Anfrage der betreffenden Person vom Auftraggeber nicht, nicht richtig oder nicht rechtzeitig beantwortet wird.

## 10 Weisungen

(1) Im Rahmen dieser Vereinbarung ist der Auftraggeber allein für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze verantwortlich, insbesondere für die Rechtmäßigkeit der Weitergabe von Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung ("Verantwortlicher" im Sinne von Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

(2) Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf eine Leistungsänderung behandelt. Bei Änderungsvorschlägen informiert der Auftragnehmer den Auftraggeber über die

Auswirkungen auf die vereinbarten Leistungen. Ist dem Auftragnehmer die Durchführung der Weisung nicht zumutbar, ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden.

## 11 Datenverarbeitung außerhalb EU/EWR

(1) Die vertraglich vereinbarte Datenverarbeitung findet in der Regel überwiegend in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Für den Fall, dass eine Übermittlung in ein Drittland erfolgt, stellt der Auftragnehmer sicher, dass die Anforderungen nach Art. 44 ff. DSGVO erfüllt sind.

(2) Der Auftraggeber gestattet die Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. Aus der Anlage ergeben sich die vom Auftraggeber genehmigten Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung.

(3) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung der Regelungen nach Art. 44 ff. DSGVO allein verantwortlich.

## 12 Haftung und Schadenersatz

(1) Für den Fall, dass eine betroffene Person einen Anspruch auf Schadensersatz gemäß Art. 82 DSGVO geltend macht, verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Klärung des zugrunde liegenden Sachverhalts beizutragen.

(2) Die zwischen den Parteien im Hauptvertrag über die Erbringung von Dienstleistungen vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter gemäß Art. 82 DSGVO, sofern nicht ausdrücklich etwas anderes vereinbart ist.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist.

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

## 13 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt.

## 14 Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

## 15 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Der Auftraggeber erkennt diese Vereinbarung als Teil der AGB https://planubo.com/de/agb/ über das von ihm gebuchte Produkt an.

(4) Der Vertrag beginnt mit dem Abschluss durch den Auftraggeber. Erfolgt eine Auftragsverarbeitung noch nach Beendigung dieser Vereinbarung, gelten die Bestimmungen dieser Vereinbarung bis zum tatsächlichen Ende der Verarbeitung.

(5) Der Auftragnehmer kann den Vertrag nach eigenem Ermessen mit angemessener Frist ändern. Insbesondere behält sich der Auftragnehmer ausdrücklich das Recht vor, diesen Vertrag einseitig zu ändern, wenn sich wesentliche rechtliche Änderungen in Bezug auf diesen Vertrag ergeben. Der Auftragnehmer wird den Auftraggeber auf die Bedeutung der geplanten Änderung gesondert hinweisen und ihm darüber hinaus eine angemessene Frist zur Erklärung eines Widerspruchs einräumen. Der Auftragnehmer wird den Auftraggeber in der Änderungsmitteilung darauf hinweisen, dass die Änderung wirksam wird, wenn der Auftraggeber nicht innerhalb der gesetzten Frist widerspricht. Im Falle eines Widerspruchs des Auftraggebers hat der Auftragnehmer ein außerordentliches Kündigungsrecht.

(6) Ausschließlicher Gerichtsstand für alle Streitigkeiten, die sich aus und im Zusammenhang mit diesem Vertrag ergeben, ist der Sitz des Auftragnehmers, soweit die Parteien Kaufleute sind. Dies gilt vorbehaltlich eines ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland und der europarechtlichen Vorschriften wie der DSGVO.

(7) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(8) Der Auftragnehmer ist berechtigt, diesen AVV zu ändern, soweit dies zur Anpassung an geänderte rechtliche Rahmenbedingungen, geänderte technische und organisatorische Maßnahmen, neue oder ausgetauschte Subunternehmer oder geänderte Funktionen der Software-Lösung erforderlich ist. Der Auftragnehmer legt dem Auftraggeber den geänderten AVV in der SaaS-Anwendung zur aktiven Zustimmung vor. Die Regelungen zur aktiven Zustimmung, zur vorübergehenden Funktionseinschränkung, zum Kündigungsrecht bei Verweigerung und zum Consent-Log aus Teil A Ziff. 1.3 und 1.4 der AGB des Anbieters gelten entsprechend.

# Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

- Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)
    - Sensible Daten, Datenbanken und Mediendateien, die hochgeladen werden, sind verschlüsselt
- Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
    - Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.
        - Der Server und die Datenbank des Auftragnehmers befinden sich in Deutschland bei der Strato AG
        - Bilder, Rechnungen und Uploads werden auf Amazon AWS S3 Buckets in Frankfurt gespeichert
    - Zugangskontrolle: Keine unbefugte Systembenutzung
        - Bestimmung des Schutzbedarfs
        - Implementierung von sicheren Zugangsverfahren und starker Authentifizierung
        - Implementierung einer einfachen Authentifizierung über Benutzernamen und Passwort
        - Sichere (verschlüsselte) Übertragung von Authentifizierungsgeheimnissen
        - Sperrung bei Fehlversuchen und Verfahren zum Zurücksetzen gesperrter Zugangskennungen
        - Bestimmung von befugten Personen
        - Verwaltung der persönlichen Authentifizierungsmedien und Zugangsberechtigungen
        - Implementierung von Zugangsbeschränkungen
        - Manuelle Zugangssperrung
    - Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
        - Zuweisung von Mindestberechtigungen
    - Mandantentrennung: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
        - Datensparsamkeit beim Umgang mit personenbezogenen Daten
        - Regelmäßige Verwendungszweckkontrolle und Löschung
        - Trennung von Test- und Entwicklungsumgebung
- Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
    - Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
        - Bestimmung der zum Empfang/zur Übermittlung von Daten berechtigten Personen
        - Überprüfung der Rechtmäßigkeit der Übermittlung ins Ausland
        - Sichere Datenübertragung zwischen Server und Client
        - Sichere Übertragung zu externen Systemen
        - Sichere Speicherung von Daten, einschließlich Backups
        - Datenschutzkonformer Lösch- und Vernichtungsprozess
    - Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

        - Protokollierung der Eingaben
        - Beweissicherung bei Online-Erteilung von SEPA-Mandaten durch unveränderliche Protokollierung von IP-Adresse, User-Agent, Zeitstempel und versioniertem Snapshot des Mandatstextes
        - Revisionssicheres Consent-Log zur Zustimmung zu AGB, Datenschutzbestimmungen und AVV: Speicherung von Nutzerkennung, E-Mail, IP, User-Agent, Zeitstempel, Sprachfassung, Dokument-URL, Versionskennung und SHA-256-Hash der zugestimmten Fassung
- Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
    - Monitoring
    - Ressourcenplanung und -bereitstellung
    - Verteidigung gegen Missbrauch des Systems
    - Datensicherungskonzepte und Umsetzung
- Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
    - Datensicherungskonzepte und Umsetzung
- Datenschutzorganisation
    - Definition von Verantwortlichkeiten
    - Implementierung und Kontrolle geeigneter Prozesse
    - Verpflichtung zur Vertraulichkeit
    - Regelungen zur internen Aufgabenverteilung
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
    - Prozess für Incident-Response-Management
        - Erkennung und Untersuchung von Sicherheitsvorfällen
    - Datenschutzfreundliche Voreinstellungen: Wenn Daten zur Erreichung des Nutzungszwecks nicht erforderlich sind, sind die technischen Voreinstellungen so definiert, dass Daten nur auf Grund einer Handlung der betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.
- Auftragskontrolle
    - Auswahl von weiteren Auftragnehmern nach geeigneten Garantien
- Lösch- und Aufbewahrungskonzept: Der Auftragnehmer verfügt über ein dokumentiertes technisches und organisatorisches Lösch- und Aufbewahrungskonzept zur Umsetzung der datenschutzrechtlichen Löschpflichten sowie gesetzlicher Aufbewahrungspflichten. Das Konzept umfasst insbesondere:
    - Verfahren zur fristgerechten Löschung bzw. Anonymisierung personenbezogener Daten,
    - Regelungen zur Berücksichtigung gesetzlicher Aufbewahrungspflichten,
    - ein abgestuftes Löschverfahren (insbesondere logische und physische Löschung),
    - Zugriffsbeschränkungen auf aufbewahrungspflichtige Daten,
    - Prozesse zur Bearbeitung von Löschanfragen betroffener Personen.

  Die konkreten Löschfristen und Datenkategorien werden im internen Lösch- und Aufbewahrungskonzept des Auftragnehmers dokumentiert und regelmäßig überprüft sowie bei Bedarf angepasst.

# Anlage 2 – Vereinbarung zur Auftragsverarbeitung - Genehmigte Subunternehmer / weitere Auftragsverarbeiter

Stand: 19-Mai-2026

| Subunternehmer | Kategorie | Kurzbeschreibung der Leistung | Standort des Unternehmens | Daten Standort | Angaben zu geeigneten Garantien |
|---|---|---|---|---|---|
| Amazon Web Services, Inc. | Hosting | Speicherung von Bildern, Rechnungen und Uploads | USA | EU (IE) | Zertifiziert unter EU-U.S. Data Privacy Framework (Angemessenheitsbeschluss) |
| Mollie B.V. | Zahlungen | Zahlungsabwicklung | NL | EU | Nicht erforderlich |
| Paddle | Zahlungen | Zahlungsabwicklung und Lizenzverwaltung | UK | Global | Angemessenheitsbeschluss |
| Strato GmbH | Hosting | Verarbeitung von Supportanfragen | DE | DE | Nicht erforderlich |
| Hetzner Online GmbH | Hosting | Hosting der SaaS-Anwendung | DE | DE | Nicht erforderlich |
| Google LLC | Kalender | Termin- und Zeitplanung | USA | Global | Zertifiziert unter EU-U.S. Data Privacy Framework (Angemessenheitsbeschluss) |
| Sendinblue GmbH (Brevo) | E-Mail | E-Mail-Versand und E-Mail Marketing | DE | EU | Nicht erforderlich |