Auftragsverarbeitungsvertrag (AVV)

gem. Art. 28 DS-GVO

---

zwischen

dem Nutzer der BASY-Kalkulation Plattform (nachfolgend **"Verantwortlicher"** oder **"Auftraggeber"**)

und

Metalldesign Weber, Andreas Weber 78467 Konstanz

nachfolgend **"Auftragsverarbeiter"** oder **"BASY"**

Präambel

Der Verantwortliche nutzt die von BASY betriebene internetbasierte SaaS-Plattform „BASY-Kalkulation" zur Kalkulation von Balkongeländern und Balkonanlagen sowie zur Verwaltung von Kundenprojekten. In diesem Zusammenhang verarbeitet BASY personenbezogene Daten im Auftrag des Verantwortlichen.

Nach Art. 28 DS-GVO ist hierfür der Abschluss eines Auftragsverarbeitungsvertrags erforderlich. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Der Verantwortliche ist für die Einhaltung der Vorschriften der DS-GVO und anderer Datenschutzvorschriften verantwortlich und behält die Herrschaft über die zu verarbeitenden Daten.

---

§ 1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung der BASY-Kalkulation Plattform, wie in **Anlage 1** näher beschrieben.

1.2 Dauer

Dieser Vertrag beginnt mit der Registrierung des Verantwortlichen auf der Plattform und läuft für die Dauer der Nutzung der BASY-Kalkulation Dienste. Er endet automatisch mit Beendigung des zugrunde liegenden Nutzungsvertrags.

---

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt zu folgenden Zwecken:

1. **Plattformbereitstellung:** Betrieb der SaaS-Anwendung zur Balkon-Kalkulation, Projektverwaltung und Materialanfrage
2. **Nutzerverwaltung:** Authentifizierung, Autorisierung und Verwaltung von Benutzerkonten
3. **Abrechnung:** Verarbeitung von Zahlungen, Erstellung von Rechnungen und Verwaltung von Abonnements
4. **Lead-Verarbeitung:** Entgegennahme und Weiterleitung von Kundenanfragen über das Balkonkonfigurator-Widget
5. **CRM-Synchronisation:** Synchronisation von Kunden- und Projektdaten mit angebundenen CRM-Systemen
6. **KI-Bildgenerierung:** Verarbeitung hochgeladener Fotos zur Erstellung von Balkon-Visualisierungen
7. **Kommunikation:** Versand von systemrelevanten Benachrichtigungen (Passwort-Reset, Kontoänderungen)

---

§ 3 Kategorien betroffener Personen

Die Verarbeitung betrifft folgende Kategorien betroffener Personen:

Kategorie	Beschreibung
Nutzer des Verantwortlichen	Mitarbeiter und Beauftragte des Verantwortlichen, die Zugang zur Plattform haben (Administratoren, Benutzer)
Endkunden des Verantwortlichen	Personen, die über das Widget des Verantwortlichen Anfragen stellen oder deren Daten im Rahmen von Kalkulationen erfasst werden
Kontaktpersonen	Ansprechpartner bei Lieferanten oder Geschäftspartnern des Verantwortlichen

---

§ 4 Art der personenbezogenen Daten

Folgende Arten personenbezogener Daten werden verarbeitet:

4.1 Stamm- und Kontaktdaten

- Vor- und Nachname
- Firmenname
- Anschrift (Straße, PLZ, Ort, Land)
- E-Mail-Adresse
- Telefonnummer

4.2 Zugangsdaten

- E-Mail-Adresse (als Login)
- Passwort-Hash (verschlüsselt gespeichert)
- Session-Tokens

4.3 Nutzungsdaten

- Kalkulationsdaten (Projektnamen, Konfigurationen, Notizen)
- Materialanfragen (Lieferadressen, Wunschtermine, Nachrichten)
- Kundennamen in Kalkulationen

4.4 Lead-Daten (Widget)

- Name, E-Mail, Telefonnummer
- Postleitzahl (Lieferort)
- Balkonkonfiguration (Maße, Anzahl, Geländerpräferenzen)
- Einwilligungszeitpunkt (DSGVO-Consent)
- Referrer-URL

4.5 Finanzdaten

- Zahlungsreferenzen (Stripe Customer-ID, Subscription-ID)
- Transaktionsbeträge
- Rechnungsnummern und -dokumente

4.6 Bilddaten

- Vom Nutzer hochgeladene Fotos (Balkone, Gebäude)
- KI-generierte Visualisierungen

4.7 Technische Daten

- IP-Adressen (Server-Logs)
- Browser- und Geräteinformationen (über Server-Logs)

Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) werden nicht verarbeitet.

---

§ 5 Pflichten des Auftragsverarbeiters

5.1 Weisungsgebundenheit

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland — es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer anderweitigen Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder andere Datenschutzvorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird.

5.2 Vertraulichkeit

a) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

b) Der Nachweis der Vertraulichkeitsverpflichtung ist dem Verantwortlichen auf Anfrage vorzulegen.

5.3 Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft alle gemäß Art. 32 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in **Anlage 3** dokumentiert. Der Auftragsverarbeiter darf die technischen und organisatorischen Maßnahmen anpassen, sofern das Sicherheitsniveau nicht unterschritten wird.

5.4 Unterstützungspflichten

a) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten (Art. 12–23 DS-GVO).

b) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Art. 32–36 DS-GVO (Sicherheit, Meldepflichten, Datenschutz-Folgenabschätzung).

5.5 Löschung und Rückgabe

Nach Beendigung der Verarbeitung löscht der Auftragsverarbeiter alle personenbezogenen Daten oder gibt sie nach Wahl des Verantwortlichen zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Pflicht zur Speicherung besteht. Die Löschung erfolgt innerhalb von 30 Tagen nach Vertragsende und wird auf Anfrage dokumentiert.

Hiervon ausgenommen sind Daten, die aufgrund gesetzlicher Aufbewahrungspflichten (insb. § 257 HGB, § 147 AO) aufbewahrt werden müssen. Diese werden für die Dauer der gesetzlichen Aufbewahrungsfrist gesperrt und nach Ablauf gelöscht.

5.6 Meldepflichten

a) Der Auftragsverarbeiter meldet dem Verantwortlichen unverzüglich jede Verletzung des Schutzes personenbezogener Daten. Die Meldung enthält mindestens:

- Beschreibung der Art der Verletzung (soweit möglich mit Angabe der Kategorien und ungefähren Zahl der betroffenen Personen und Datensätze)

- Name und Kontaktdaten der Anlaufstelle für weitere Informationen
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Maßnahmen von Aufsichtsbehörden (Art. 58 DS-GVO), die auch die im Auftrag verarbeiteten Daten betreffen können.

---

§ 6 Rechte und Pflichten des Verantwortlichen

a) Der Verantwortliche ist als Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte allein verantwortlich.

b) Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen können in Textform (z.B. per E-Mail) erfolgen.

c) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten feststellt.

d) Für die Erfüllung der Meldepflichten nach Art. 33, 34 DS-GVO ist der Verantwortliche verantwortlich.

---

§ 7 Kontrollrechte des Verantwortlichen

a) Der Verantwortliche hat das Recht, die Einhaltung der datenschutzrechtlichen Vorschriften und dieses Vertrags durch den Auftragsverarbeiter zu kontrollieren.

b) Der Auftragsverarbeiter ist zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle erforderlich ist.

c) Kontrollen vor Ort können nach vorheriger Anmeldung mit angemessener Frist (mindestens 30 Tage) zu den üblichen Geschäftszeiten durchgeführt werden, höchstens einmal jährlich. Zusätzliche Kontrollen sind nur bei begründetem Anlass möglich.

d) Der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen kann alternativ durch Vorlage geeigneter Zertifizierungen, Testate oder Prüfberichte unabhängiger Stellen erbracht werden.

---

§ 8 Unterauftragsverarbeiter

8.1 Genehmigte Unterauftragsverarbeiter

Der Verantwortliche stimmt dem Einsatz der in **Anlage 2** aufgeführten Unterauftragsverarbeiter zu. Der Auftragsverarbeiter hat mit jedem Unterauftragsverarbeiter einen Auftragsverarbeitungsvertrag geschlossen, der den Anforderungen des Art. 28 DS-GVO entspricht.

8.2 Änderungen bei Unterauftragsverarbeitern

a) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 4 Wochen vor dem geplanten Einsatz eines neuen oder dem Wechsel eines bestehenden Unterauftragsverarbeiters in Textform.

b) Der Verantwortliche kann dem Einsatz innerhalb von 14 Tagen nach Zugang der Information unter Angabe einer Begründung widersprechen. Erfolgt kein Widerspruch, gilt dies als Zustimmung.

c) Im Falle eines berechtigten Widerspruchs bemühen sich die Parteien, eine einvernehmliche Lösung zu finden. Gelingt dies nicht, kann der Verantwortliche den Vertrag mit einer Frist von 30 Tagen kündigen.

8.3 Pflichten gegenüber Unterauftragsverarbeitern

Der Auftragsverarbeiter stellt sicher, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragsverarbeitern gelten, insbesondere die Kontrollbefugnisse des Verantwortlichen und der Aufsichtsbehörden.

---

§ 9 Drittlandtransfer

9.1 Allgemeines

Eine Übermittlung personenbezogener Daten in Drittländer (Staaten außerhalb des EWR) erfolgt nur, sofern die besonderen Voraussetzungen der Art. 44–49 DS-GVO erfüllt sind.

9.2 Absicherung der Drittlandtransfers

Für die in Anlage 2 aufgeführten Unterauftragsverarbeiter mit Sitz in den USA gelten folgende Absicherungen:

Mechanismus	Anwendung
EU-US Data Privacy Framework (DPF)	Für Unterauftragsverarbeiter mit gültiger DPF-Zertifizierung (Supabase, Stripe, Vercel, OpenAI, Airtable)
Standardvertragsklauseln (SCCs)	Als Rückfall-Mechanismus gemäß Durchführungsbeschluss (EU) 2021/914, falls DPF ungültig wird
Ergänzende Maßnahmen	Verschlüsselung in Transit (TLS) und at Rest, Pseudonymisierung wo möglich, Zugriffsbeschränkungen

9.3 Kein Drittlandtransfer

Folgende Unterauftragsverarbeiter verarbeiten Daten ausschließlich innerhalb der EU/des EWR:

- **easybill GmbH** (Deutschland) — verpflichtet sich vertraglich zur Verarbeitung nur in EU/EWR
- **Make.com / Celonis SE** (EU-Rechenzentren) — bei Drittlandtransfer greifen DPF + SCCs

---

§ 10 Wahrung von Betroffenenrechten

a) Der Verantwortliche ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Anfragen von Betroffenen, die bei ihm eingehen.

b) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung von Anträgen auf:

- Auskunft (Art. 15 DS-GVO)
- Berichtigung (Art. 16 DS-GVO)
- Löschung (Art. 17 DS-GVO)
- Einschränkung der Verarbeitung (Art. 18 DS-GVO)
- Datenübertragbarkeit (Art. 20 DS-GVO)
- Widerspruch (Art. 21 DS-GVO)

c) Der Auftragsverarbeiter beantwortet Anfragen von Betroffenen nicht selbst, es sei denn, er wird hierzu vom Verantwortlichen autorisiert.

---

§ 11 Vergütung

Unterstützungsleistungen des Auftragsverarbeiters bei der Erfüllung von Betroffenenrechten und Audits, die über die normale Nutzung der Plattform hinausgehen, können gesondert vergütet werden. Die Parteien vereinbaren hierzu im Einzelfall angemessene Konditionen.

---

§ 12 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DS-GVO. Im Übrigen gelten die Haftungsregelungen des zugrunde liegenden Nutzungsvertrags.

---

§ 13 Schlussbestimmungen

a) Dieser Vertrag unterliegt deutschem Recht.

b) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform.

c) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

d) Im Falle von Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag gehen die Regelungen dieses Vertrags vor.

Anlage 1: Beschreibung der Verarbeitungstätigkeit

Gegenstand der Verarbeitung

Bereitstellung einer SaaS-Plattform zur Kalkulation von Balkongeländern und Balkonanlagen, einschließlich Projektverwaltung, Materialanfragen, Lead-Management, Abrechnung und KI-gestützter Bildgenerierung.

Art der Verarbeitung

Erheben, Speichern, Verändern, Auslesen, Abfragen, Verwenden, Übermitteln (an genehmigte Unterauftragsverarbeiter), Löschen von personenbezogenen Daten im Rahmen der Plattformnutzung.

Zweck der Verarbeitung

- Bereitstellung und Betrieb der BASY-Kalkulation Plattform
- Verwaltung von Benutzerkonten und Berechtigungen
- Durchführung von Kalkulationen und Projektverwaltung
- Verarbeitung von Kundenanfragen (Leads) über das Widget
- Abwicklung von Zahlungen und Rechnungsstellung
- Synchronisation mit CRM-Systemen des Verantwortlichen
- KI-gestützte Visualisierung von Balkonanlagen

Kategorien betroffener Personen

Siehe § 3 dieses Vertrags.

Art der personenbezogenen Daten

Siehe § 4 dieses Vertrags.

Anlage 2: Genehmigte Unterauftragsverarbeiter

Übersicht

Nr.	Unterauftragsverarbeiter	Sitz	Zweck	Verarbeitungsort	DPA/AVV
1	**Supabase, Inc.**	San Francisco,	Datenbank, Authentifizierung,	EU (Frankfurt)	Supabase DPA

		CA, USA	Dateispeicherung		
2	**Stripe, Inc.**	San Francisco, CA, USA	Zahlungsabwicklung, Abonnementverwaltung	EU + Global	Stripe DPA
3	**easybill GmbH**	Düsselstr. 21, 41564 Kaarst, DE	Rechnungserstellung, Dokumentenverwaltung	Deutschland (EU/EWR)	easybill AVV v1.2.2
4	**Celonis SE (Make.com)**	Thomas-Dehler-Str. 27, 80737 München, DE	Workflow-Automatisierung (EasyBill-Kundenerstellung)	EU	Celonis DPA for Make (Mai 2024)
5	**Airtable, Inc.**	San Francisco, CA, USA	CRM-Datensynchronisation	USA	Airtable DPA
6	**OpenAI, L.L.C.**	San Francisco, CA, USA	KI-Bildgenerierung (DALL-E)	USA	OpenAI DPA
7	**Vercel, Inc.**	San Francisco, CA, USA	Application Hosting, Serverless Functions	EU (Frankfurt)	Vercel DPA

Details zu den Unterauftragsverarbeitern

1. Supabase, Inc.

- **Verarbeitete Daten:** Alle in § 4 genannten Datenkategorien (Datenbank), Authentifizierungsdaten (Auth), hochgeladene Dateien und Rechnungs-PDFs (Storage)
- **Absicherung Drittlandtransfer:** EU-US Data Privacy Framework, SCCs als Rückfall
- **Eigene Sub-Processors:** AWS (Amazon Web Services) für Infrastruktur

2. Stripe, Inc.

- **Verarbeitete Daten:** Firmenname, E-Mail-Adresse, Zahlungsreferenzen, Transaktionsbeträge, Abonnementdaten. Zahlungskartendaten werden ausschließlich von Stripe verarbeitet und berühren nie die BASY-Server.
- **Absicherung Drittlandtransfer:** EU-US Data Privacy Framework, SCCs als Rückfall
- **Besonderheit:** Stripe ist für Kartendaten eigenständiger Verantwortlicher (PCI DSS Level 1 zertifiziert)

3. easybill GmbH

- **Verarbeitete Daten:** Firmenname, Anschrift, E-Mail-Adresse, Rechnungspositionen (Plan-Bezeichnung, Beträge), Rechnungsnummern
- **Verarbeitungsort:** Ausschließlich EU/EWR (vertraglich zugesichert, § 4b easybill AVV)
- **Eigene Unterauftragnehmer (gem. easybill AVV Anlage 2):**
  - Hetzner Online GmbH, Gunzenhausen (Webhosting)
  - DocuSystem GmbH, Rödermark (Rechnungsdruck)
  - GTC TeleCommunication GmbH, Stuttgart (Faxversand)
  - Amazon.com Inc., USA (Datensicherung — Serverstandort Deutschland, AES-256 verschlüsselt)

4. Celonis SE (Make.com)

- **Verarbeitete Daten:** Firmenname, Anschrift des Verantwortlichen (zur EasyBill-Kundenerstellung), EasyBill-Customer-IDs

- **Absicherung Drittlandtransfer:** DPF als primärer Mechanismus, SCCs (Modul 2: Controller-to-Processor) als Rückfall gemäß Durchführungsbeschluss (EU) 2021/914
- **Eigene Sub-Processors:** Gelistet unter https://www.make.com/en/terms-and-conditions
- **TOMs:** Dokumentiert unter https://www.make.com/en/technical-and-organizational-measures
- **Datenlöschung:** Innerhalb von 30 Tagen nach Vertragsende (Abschnitt 3.3 Make DPA)
- **Audit-Kontakt:** isms@celonis.com

5. **Airtable, Inc.**
   - **Verarbeitete Daten:** Firmenname, Anschrift, E-Mail, Kundentyp, Plan-Status, EasyBill-Customer-ID, Tenant-ID, Kontaktdaten, Projektdaten
   - **Absicherung Drittlandtransfer:** EU-US Data Privacy Framework, SCCs als Rückfall

6. **OpenAI, L.L.C.**
   - **Verarbeitete Daten:** Vom Nutzer hochgeladene Fotos, Textprompts (Beschreibungen), generierte Bilder
   - **Absicherung Drittlandtransfer:** EU-US Data Privacy Framework, SCCs als Rückfall
   - **Besonderheit:** Es werden keine personenbezogenen Daten (Namen, Adressen etc.) an OpenAI übermittelt — nur Bilddaten und Textbeschreibungen. Fotos können jedoch Gebäude oder Personen zeigen.

7. **Vercel, Inc.**
   - **Verarbeitete Daten:** Alle Daten in Transit (Anfragen an die Plattform), Server-Logs (IP-Adressen, Zeitstempel), Cron-Job-Ausführungen
   - **Absicherung Drittlandtransfer:** EU-US Data Privacy Framework, SCCs als Rückfall
   - **Deployment-Region:** EU (Frankfurt)

Anlage 3: Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter trifft folgende technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO:

1. Vertraulichkeit

a) Zutrittskontrolle

- Keine eigenen physischen Server — alle Daten in Managed-Cloud-Rechenzentren (Supabase/AWS, Vercel) mit ISO 27001 Zertifizierung
- Zugang zur Cloud-Infrastruktur ausschließlich über authentifizierte und autorisierte Zugänge

b) Zugangskontrolle

- Authentifizierung über E-Mail und Passwort mit sicherer Passwort-Hashing (bcrypt via Supabase Auth)
- Session-Management über JWT-Tokens in httpOnly, Secure, SameSite Cookies
- API-Zugriff über signierte Tokens und API-Keys
- Separate Service-Role-Keys für administrative Server-Operationen (nie im Client exponiert)

c) Zugriffskontrolle

- Rollenbasiertes Berechtigungskonzept (RBAC) mit drei Rollen: Superadmin, Partner-Admin, Partner-Benutzer
- Row-Level Security (RLS) auf Datenbankebene — jeder Datensatz ist einem Mandanten zugeordnet
- Strikte Mandantentrennung über `tenant_id` auf allen Tabellen
- Protokollierung von Datenbankzugriffen über Supabase Audit-Logs

d) Trennungskontrolle

- Logische Trennung der Mandantendaten durch `tenant_id` auf allen Datenbankebenen
- Separate Authentifizierung und Autorisierung pro Mandant
- Getrennte Speicherbereiche (Storage Buckets) pro Mandant für Rechnungs-PDFs

2. Integrität

a) Eingabekontrolle

- Serverseitige Validierung aller Eingaben durch Zod-Schema-Validierung
- Protokollierung von Datenänderungen über Zeitstempel (`created_at` , `updated_at`)
- Nachvollziehbarkeit durch `created_by` -Felder auf relevanten Tabellen

b) Weitergabekontrolle

- Verschlüsselung aller Datenübertragungen über TLS 1.2+ (HTTPS)
- Webhook-Signaturprüfung für eingehende Daten (Stripe: HMAC-SHA256, Airtable: timingSafeEqual mit Webhook-Secret)
- API-Keys und Secrets werden ausschließlich serverseitig verwendet und in verschlüsselten Umgebungsvariablen gespeichert

3. Verfügbarkeit und Belastbarkeit

- Hosting auf Vercel mit automatischem Failover und globaler CDN-Verteilung
- Supabase Managed Database mit automatischen Backups und Point-in-Time Recovery
- Redundante Datenspeicherung durch den Cloud-Anbieter (AWS)
- Monitoring und Alerting über Vercel Dashboard und Supabase Logs

4. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung der Zugriffskontrollmechanismen
- Dependency-Audits über automatisierte Security-Scanner (npm audit)
- Regelmäßige Aktualisierung von Abhängigkeiten und Sicherheitspatches
- Supabase Security Advisors für automatische Schwachstellenerkennung (fehlende RLS-Policies, Performance-Probleme)

Anlage 4: Cookies und Tracking

Eingesetzte Cookies

Cookie	Zweck	Typ	Dauer	httpOnly	Secure
`sb-access-token`	Supabase Auth JWT	Funktional (erforderlich)	Session	Ja	Ja
`sb-refresh-token`	Supabase Session-Refresh	Funktional (erforderlich)	Konfigurierbar	Ja	Ja

Tracking und Analyse

- Es werden **keine** Third-Party-Analytics-Dienste eingesetzt (kein Google Analytics, kein Matomo, keine Tracking-Pixel)
- Es werden **keine** Marketing-Cookies gesetzt
- Das Widget erfasst die `referrer_url` zur Nachverfolgung der Lead-Quelle — dies dient ausschließlich dem Verantwortlichen zur Zuordnung seiner Leads

---

Anlage 5: Aufbewahrungsfristen und Löschkonzept

Datenkategorie	Aufbewahrungsfrist	Rechtsgrundlage	Löschmethode
Rechnungen / Plan-Transaktionen	10 Jahre nach Erstellung	§ 257 HGB, § 147 AO	Automatische Löschung nach Fristablauf

Nutzerdaten nach Kontolöschung	30 Tage	Art. 17 DS-GVO	Hard-Delete aus Datenbank
Widget-Leads ohne Conversion	6 Monate	Zweckbindung (Art. 5 Abs. 1b DS-GVO)	Automatische Löschung
KI-Bilder	12 Monate nach letztem Zugriff	Speicherbegrenzung	Automatische Löschung aus Storage
Server-Logs (IP-Adressen)	90 Tage	Berechtigtes Interesse (Art. 6 Abs. 1f)	Automatische Log-Rotation
Kalkulationsdaten nach Kontolöschung	30 Tage	Art. 17 DS-GVO	Hard-Delete aus Datenbank

Hinweis: Die technische Umsetzung der automatisierten Löschfristen wird schrittweise implementiert. Bis zur vollständigen Automatisierung erfolgt die Löschung auf dokumentierte Anfrage des Verantwortlichen.

Unterschriften

Auftragsverarbeiter:

Ort, Datum: Konstanz, 20.02.2026

Name: Andreas Weber Unterschrift: 

Verantwortlicher:

Ort, Datum: _____

Name: _____ Firma: _____ Unterschrift: _____

Version 1.0 — Stand: Februar 2026