

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

für die Nutzung von HACCP Control

Version 1.0, Stand: September 2026

Diese Vereinbarung wird geschlossen zwischen dem Betrieb, der HACCP Control nutzt (nachfolgend „Auftraggeber“), und der FORMM Media & Marketing UG (haftungsbeschränkt), Edisonstrasse 63, 12459 Berlin, vertreten durch den Geschäftsführer Simon Forstemann (nachfolgend „Auftragnehmer“).

Sie konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus dem Nutzungsvertrag über HACCP Control (Allgemeine Geschäftsbedingungen, nachfolgend „Nutzungsvertrag“). Sie gilt, soweit der Auftraggeber in HACCP Control personenbezogene Daten verarbeitet, für die er Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist, insbesondere Daten seiner Beschäftigten.

Die Vereinbarung wird mit der Registrierung oder der ersten Nutzung von HACCP Control in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Sie ist unter haccp-control.com/avv abrufbar und kann als PDF gespeichert werden. Auf Wunsch zeichnet der Auftragnehmer eine vom Auftraggeber unterschriebene Fassung gegen.

§ 1 Gegenstand und Dauer

(1) Gegenstand der Verarbeitung ist die Bereitstellung und der Betrieb der Web-Anwendung HACCP Control zur Dokumentation der betrieblichen Eigenkontrolle: Checklisten, Temperaturprotokolle, Reinigungs- und Arbeitspläne, HACCP-Konzept, Schulungsverwaltung und Team-Schulungen, einschließlich Speicherung, Synchronisation zwischen Geräten, Auswertung, Erstellung von PDF-Dokumenten, Export und Versand von Benachrichtigungen.

(2) Die Vereinbarung gilt für die Dauer des Nutzungsvertrags. Sie endet mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten nach § 8 (Löschung und Rückgabe) bleiben davon unberührt.

§ 2 Art und Zweck der Verarbeitung, Datenarten, betroffene Personen

Art und Zweck der Verarbeitung, die Arten der personenbezogenen Daten und die Kategorien der betroffenen Personen ergeben sich aus Anlage 1. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand dieser Vereinbarung; der Auftraggeber trägt solche Daten nicht in die Anwendung ein.

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich im Rahmen dieser Vereinbarung und auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Die Weisungen sind durch den Nutzungsvertrag und die Funktionen der Anwendung, die der Auftraggeber verwendet, festgelegt. Jede Eingabe, Freigabe, Exportanforderung oder Löschung in der Anwendung gilt als Weisung.

(2) Ergänzende Weisungen erteilt der Auftraggeber in Textform, in der Regel per E-Mail an hallo@haccp-control.com. Mündlich erteilte Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(3) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

(4) Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt. Unberührt bleibt eine Verarbeitung, zu der der Auftragnehmer nach dem Recht der Union oder eines Mitgliedstaats verpflichtet ist; in diesem Fall teilt er dem Auftraggeber die rechtliche Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 4 Pflichten des Auftragnehmers

(1) Vertraulichkeit. Der Auftragnehmer verpflichtet alle mit der Verarbeitung befassten Personen zur Vertraulichkeit (Art. 28 Abs. 3 Satz 2 lit. b, Art. 29 DSGVO) und unterrichtet sie über die Pflichten aus dieser Vereinbarung. Die Vertraulichkeitspflicht besteht auch nach Beendigung der Tätigkeit fort.

(2) Sicherheit der Verarbeitung. Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie auf dem Stand der Technik. Er darf sie weiterentwickeln, solange das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er in Anlage 2.

(3) Rechte betroffener Personen. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Mitteln bei der Erfüllung der Rechte betroffener Personen nach Art. 12 bis 22 DSGVO, insbesondere durch die Export-Funktion der Anwendung (Auskunft, Datenübertragbarkeit) sowie durch Berichtigung und Löschung von Daten auf Weisung. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er das Ersuchen unverzüglich an den Auftraggeber weiter und beantwortet es nicht ohne dessen Weisung.

(4) Verletzungen des Schutzes personenbezogener Daten. Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die die Verarbeitung nach dieser Vereinbarung betrifft, unverzüglich nach Kenntnis, in der Regel innerhalb von 48 Stunden, mit den ihm vorliegenden Angaben nach Art. 33 Abs. 3 DSGVO. Er unterstützt den Auftraggeber bei dessen Pflichten aus Art. 33 und 34 DSGVO.

(5) Weitere Unterstützung. Der Auftragnehmer unterstützt den Auftraggeber mit den ihm verfügbaren Informationen bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der Aufsichtsbehörde (Art. 35 und 36 DSGVO).

(6) Verzeichnis. Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(7) Datenschutzbeauftragter. Der Auftragnehmer ist zur Benennung eines Datenschutzbeauftragten nicht verpflichtet. Ansprechpartner für den Datenschutz ist die Geschäftsführung, erreichbar unter hallo@haccp-control.com.

(8) Verarbeitungsort. Datenbank und Authentifizierung werden in der Europäischen Union betrieben (Amazon Web Services, Region Irland). Die Auslieferung der Anwendung, die Ausführung der Serverfunktionen und der Versand von E-Mails laufen über Dienstleister mit Sitz in den USA; dabei können personenbezogene Daten in die USA übermittelt und dort verarbeitet werden. Grundlage sind die EU-Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO. Einzelheiten stehen in Anlage 3.

§ 5 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt eine allgemeine Genehmigung für die Einschaltung der in Anlage 3 genannten Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO).

(2) Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert er den Auftraggeber mindestens vier Wochen vorher per E-Mail an die im Nutzerkonto hinterlegte Adresse und aktualisiert Anlage 3 unter haccp-control.com/avv. Der Auftraggeber kann der Änderung innerhalb von vier Wochen aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Kommt keine einvernehmliche Lösung zustande, kann jede Partei den Nutzungsvertrag zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.

(3) Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO), insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Er bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.

(4) Nebenleistungen wie Telekommunikation, Wartung ohne Zugriff auf personenbezogene Daten oder die Entsorgung von Datenträgern sind keine Unterauftragsverarbeitung im Sinne dieser Vereinbarung.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber ist als Verantwortlicher für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er informiert insbesondere seine Beschäftigten über die Verarbeitung ihrer Daten in HACCP Control (Art. 13 DSGVO) und beachtet die für ihn geltenden arbeits- und betriebsverfassungsrechtlichen Vorgaben.

(2) Der Auftraggeber erteilt Weisungen nach § 3, vergibt Rollen und Rechte in der Anwendung eigenverantwortlich und bewahrt seine Zugangsdaten sowie die PIN seiner Mitglieder sicher auf.

(3) Stellt der Auftraggeber Fehler oder Unregelmäßigkeiten bei der Verarbeitung fest, informiert er den Auftragnehmer unverzüglich.

§ 7 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Dazu gehören diese Vereinbarung mit ihren Anlagen, die Beschreibung der technischen und organisatorischen Maßnahmen sowie, soweit vorhanden, aktuelle Nachweise und Zertifizierungen der Unterauftragsverarbeiter.

(2) Genügen diese Nachweise im Einzelfall nicht, kann der Auftraggeber nach vorheriger Abstimmung, in der Regel mit einer Ankündigungsfrist von vier Wochen und während der üblichen Geschäftszeiten, Überprüfungen einschließlich Inspektionen selbst durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, höchstens einmal je Kalenderjahr, sofern kein konkreter Anlass besteht. Störungen des Geschäftsbetriebs des Auftragnehmers sind zu vermeiden.

(3) Der Auftragnehmer unterstützt Prüfungen der zuständigen Aufsichtsbehörde beim Auftraggeber, soweit sie die Verarbeitung nach dieser Vereinbarung betreffen.

§ 8 Löschung und Rückgabe

(1) Der Auftraggeber kann seine Daten jederzeit über die Export-Funktion der Anwendung (JSON) und über die PDF-Ausgaben sichern.

(2) Nach Beendigung des Nutzungsvertrags oder auf Weisung des Auftraggebers löscht der

Auftragnehmer alle personenbezogenen Daten des Auftraggebers innerhalb von 30 Tagen, sofern nicht eine Aufbewahrungspflicht nach dem Recht der Union oder eines Mitgliedstaats entgegensteht. Die Löschung verlangt der Auftraggeber per E-Mail an hallo@haccp-control.com; der Auftragnehmer bestätigt sie in Textform.

(3) In Sicherungskopien der Unterauftragsverarbeiter werden die Daten nach deren Sicherungszyklen überschrieben, spätestens 30 Tage nach der Löschung.

(4) Teilnahmebescheinigungen aus Team-Schulungen bleiben zum Nachweis der Schulung gespeichert, bis der Auftraggeber sie im Team-Dashboard widerruft oder ihre Löschung verlangt. Ein Widerruf kennzeichnet die Bescheinigung als ungültig; die Löschung erfolgt nach Absatz 2.

(5) Unterlagen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, darf der Auftragnehmer über das Vertragsende hinaus entsprechend den jeweiligen Aufbewahrungsfristen aufbewahren.

§ 9 Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Nutzungsvertrags (§ 3 der Allgemeinen Geschäftsbedingungen).

§ 10 Schlussbestimmungen

(1) In Fragen des Datenschutzes gehen die Regelungen dieser Vereinbarung denen des Nutzungsvertrags vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Der Auftragnehmer kann die Vereinbarung anpassen, wenn Gesetz, Rechtsprechung oder der Leistungsumfang dies erfordern; § 10 des Nutzungsvertrags gilt entsprechend (Information mindestens sechs Wochen vor dem Inkrafttreten, Widerspruchsrecht des Auftraggebers).

(3) Es gilt das Recht der Bundesrepublik Deutschland. Sollte eine Bestimmung dieser Vereinbarung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlagen

Anlage 1: Gegenstand der Verarbeitung

Art und Zweck der Verarbeitung:

- Speicherung, Anzeige und Synchronisation der Betriebsdaten zwischen den Geräten des Auftraggebers.
- Auswertung der Aufzeichnungen (Fälligkeiten, Abweichungen, Übersichten).
- Erstellung von PDF-Dokumenten: Kontrollordner, HACCP-Konzept, Reinigungs- und Arbeitspläne, Protokollauszüge, Teilnahmebescheinigungen.
- Export der Betriebsdaten (JSON) auf Anforderung des Auftraggebers.
- Versand von Benachrichtigungen und Erinnerungen per E-Mail an die hinterlegten Adressen.
- Ausstellung, Widerruf und Verifikation von Teilnahmebescheinigungen aus Team-Schulungen.

Kategorien betroffener Personen:

- Beschäftigte und sonstige Mitarbeitende des Auftraggebers, einschließlich Aushilfen.
- Inhaber und Ansprechpartner des Auftraggebers.

- Dritte, die in Aufzeichnungen genannt werden, etwa Lieferanten oder Prüfer.

Arten personenbezogener Daten:

- Kontakt- und Kontodaten des Auftraggebers und seiner Nutzer: Name, E-Mail-Adresse, Betriebsname, Anschrift.
- Mitgliederdaten in der Anwendung: Name, Rolle, PIN (nur als Hash).
- Aufzeichnungen der Eigenkontrolle mit Zeitstempel und Name der erfassenden Person: Temperaturen, Reinigungen, Wareneingänge, Schädlingsmonitoring, Checklisten, Korrekturmaßnahmen.
- Schulungsnachweise aus Team-Schulungen: Name, Geburtsdatum (nur zur Unterscheidung gleichnamiger Teilnehmender), Schulungsdatum, Testergebnis, Sprache, Bescheinigungsnummer.
- Nutzungs- und Protokolldaten: Zeitpunkte von Anmeldungen und Änderungen, IP-Adressen in den Serverprotokollen der Dienstleister.

Dauer der Verarbeitung: Laufzeit des Nutzungsvertrags, anschließend Löschung nach § 8.

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

1. Vertraulichkeit

- Zugangskontrolle: Anmeldung mit E-Mail-Adresse und Passwort. Passwörter werden beim Authentifizierungsdienst nur als Hash gespeichert. Das Zurücksetzen des Passworts ist nur über einen Link an die hinterlegte E-Mail-Adresse möglich. Sitzungen laufen über zeitlich befristete Token.
- Rollen und Rechte: Inhaber, Admin und Mitglied mit abgestuften Rechten. Auswertungen, Export, Abo und Verwaltung sind Inhabern und Admins vorbehalten. Optionale PIN je Mitglied, gespeichert als Hash mit Salt, nie im Klartext und nicht im Export enthalten.
- Mandantentrennung: Jeder Datensatz ist einem Betrieb zugeordnet. Zugriffsregeln auf Datenbankebene (Row Level Security) lassen ausschließlich Zugriffe des eigenen Betriebs zu.
- Administrationszugänge: auf die Geschäftsführung des Auftragnehmers beschränkt. Schlüssel und Zugangsdaten der Dienstleister werden in der Geheimnisverwaltung der Hosting-Plattform gespeichert.
- Verschlüsselung: Übertragung ausschließlich über TLS (HTTPS). Speicherung beim Datenbankanbieter verschlüsselt (AES-256), einschließlich der Sicherungskopien.

2. Integrität

- Eingabekontrolle: Jeder Protokolleintrag trägt Zeitstempel und erfassende Person (Mitglied oder PIN). Einträge sind nach dem Speichern unveränderlich; Korrekturen werden als neue Einträge dokumentiert. Schulungsnachweise sind unveränderlich und werden bei Widerruf gekennzeichnet, nicht überschrieben.
- Weitergabekontrolle: Zugriff nur über verschlüsselte Verbindungen. Export der Betriebsdaten nur durch Inhaber und Admins. E-Mail-Versand nur an hinterlegte Adressen.

3. Verfügbarkeit und Belastbarkeit

- Datensicherung: regelmäßige Sicherungen der Datenbank durch den Datenbankanbieter nach dessen Leistungsbeschreibung. Zusätzlich Export-Funktion (JSON) und PDF-Ausgaben für eigene Sicherungen des Auftraggebers.
- Offline-Betrieb: Die Anwendung hält eine lokale Kopie der Betriebsdaten auf dem Endgerät und

synchronisiert bei bestehender Verbindung. Ein Ausfall der Verbindung führt nicht zu Datenverlust.

- Infrastruktur: Betrieb in Rechenzentren von Amazon Web Services (Datenbank, Irland) und Vercel (Anwendung) mit redundanter Auslegung nach den Angaben der Anbieter.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Automatisierte Tests und Typprüfung vor jeder Veröffentlichung. Veröffentlichungen nur nach festem Freigabeverfahren mit Sicherung des vorherigen Stands.
- Regelmäßige Sicherheitsprüfungen der Anwendung und der Datenbankrechte, zuletzt im September 2026.
- Meldeprozess für Verletzungen des Schutzes personenbezogener Daten nach § 4 Abs. 4 dieser Vereinbarung.
- Auftragskontrolle: Auswahl der Unterauftragsverarbeiter nach deren Sicherheitsnachweisen (etwa SOC 2 oder ISO 27001) und Abschluss von Auftragsverarbeitungsverträgen mit ihnen.

Anlage 3: Unterauftragsverarbeiter (Stand September 2026)

- Supabase Inc. (USA): Datenbank, Authentifizierung und Dateispeicher. Hosting bei Amazon Web Services in der Region eu-west-1 (Irland); Zugriff aus den USA nur für Betrieb und Support des Anbieters. Grundlage der Übermittlung: EU-Standardvertragsklauseln als Bestandteil des Auftragsverarbeitungsvertrags mit Supabase.
- Vercel Inc. (USA): Hosting der Webanwendung, Auslieferung über ein weltweites Netz (CDN) und Ausführung der Serverfunktionen in einem Rechenzentrum in den USA. Grundlage: EU-Standardvertragsklauseln.
- Resend Inc. (USA): Versand von System-E-Mails (Bestätigungen, Erinnerungen, Zugangslinks, Bescheinigungen) an die hinterlegten Adressen. Grundlage: EU-Standardvertragsklauseln.
- Stripe Payments Europe, Ltd. (Irland): Zahlungsabwicklung und Rechnungsstellung gegenüber dem Auftraggeber. Verarbeitet nur Daten des Auftraggebers als Kunde (Name, Anschrift, Zahlungsdaten), keine Beschäftigtendaten.

Keine Unterauftragsverarbeiter im Sinne dieser Vereinbarung sind Google Ireland Ltd. und Microsoft Ireland Operations Ltd. (Reichweiten- und Werbemessung auf den öffentlichen Seiten und in der Anwendung). Dafür ist der Auftragnehmer selbst Verantwortlicher; Einzelheiten stehen in der Datenschutzerklärung, Abschnitte 5 bis 7.

Unterschriften (optional)

Diese Vereinbarung gilt mit der Registrierung als geschlossen. Wer eine gegengezeichnete Fassung braucht, unterschreibt das PDF und schickt es an hallo@haccp-control.com. Der Auftragnehmer zeichnet gegen und sendet es zurück.

Auftraggeber (Betrieb, Firmenname)

Auftragnehmer: FORMM Media & Marketing UG

Ort, Datum, Unterschrift, Name in Druckbuchstaben

Ort, Datum, Unterschrift, Name in Druckbuchstaben