VORLAGE – VOR VERWENDUNG JURISTISCH PRÜFEN LASSEN

Dieses Muster ist ein Entwurf und kein Rechtsrat. Alle Angaben in [eckigen Klammern] sind Platzhalter bzw. Vorschläge, die vor Abschluss zu ersetzen oder zu bestätigen sind. Anhang 3 enthält Angaben, die mit „Zu prüfen“ gekennzeichnet sind.

DINETAILOR · MUSTER · VERSION 0.1 · STAND 21. OKTOBER 2026

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

VERANTWORTLICHER (AUFTRAGGEBER)

[Firma und Rechtsform des Betriebs]
[Anschrift]
[Firmenbuchnummer / Handelsregister, UID]
vertreten durch [Name, Funktion]
Datenschutz-Kontakt: [E-Mail]

AUFTRAGSVERARBEITER (AUFTRAGNEHMER)

[Betreibergesellschaft von DineTailor, Rechtsform]
[Anschrift]
[Firmenbuchnummer, UID]
vertreten durch [Name, Funktion]
Datenschutz-Kontakt: [E-Mail, z. B. datenschutz@…]

Präambel

Die Parteien haben einen Vertrag über die Nutzung der Plattform DineTailor („Hauptvertrag“) geschlossen. Zur Erfüllung des Hauptvertrags verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Diese Vereinbarung konkretisiert die Rechte und Pflichten der Parteien nach Art. 28 DSGVO.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

(1) Gegenstand ist die Bereitstellung der Plattform DineTailor als Software as a Service für Reservierung, Gästeverwaltung, Bestellaufnahme und Kasse, Küche und Warenwirtschaft, Personalplanung und Zeiterfassung sowie Buchhaltungs- und Fiskalfunktionen, einschließlich des Hostings der Daten.

(2) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anhang 1.

(3) Die Vereinbarung gilt für die Laufzeit des Hauptvertrags. Die Pflichten nach § 8 gelten darüber hinaus bis zur vollständigen Löschung oder Rückgabe.

(4) [Optional, juristisch prüfen:] Für Konto- und Abrechnungsdaten der Nutzer des Verantwortlichen sowie für technische Betriebs- und Sicherheitsdaten ist der Auftragsverarbeiter eigener Verantwortlicher; diese Daten sind nicht Gegenstand dieser Vereinbarung.

§ 2 Weisungen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO), auch hinsichtlich der Übermittlung in ein Drittland, es sei denn, er ist durch Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dies dem Verantwortlichen vorab mit, soweit das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Hauptvertrag, diese Vereinbarung sowie die Nutzung und Konfiguration der Funktionen der Plattform durch den Verantwortlichen gelten als Weisung. Weitere Weisungen erteilt der Verantwortliche in Textform an [Kontakt des Auftragsverarbeiters].

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Ansicht ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Er darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.

(4) **KI-Funktionen.** Der Auftragsverarbeiter bindet KI-Funktionen in der Werkseinstellung an Anbieter mit EU-Endpunkt (Anhang 3). Stellt er eine Funktion, die personenbezogene Daten des Verantwortlichen verarbeitet, auf einen Anbieter außerhalb der EU um, geschieht das nur nach dokumentierter Entscheidung (Begründung, Bestätigung, Audit-Eintrag). Der Auftragsverarbeiter informiert den Verantwortlichen darüber [Frist und Verfahren festlegen]; der Verantwortliche kann widersprechen, [Rechtsfolge bei Widerspruch festlegen]. Die Lieferschein-Erkennung ist eine feste Ausnahme (§ 5 Abs. 3).

§ 3 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit.** Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO).

(2) **Sicherheit.** Der Auftragsverarbeiter trifft die in Anhang 2 beschriebenen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO). Er darf sie weiterentwickeln, solange das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er.

(3) **Betroffenenrechte.** Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anfragen betroffener Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 lit. e), insbesondere durch Export-, Berichtigungs- und Löschfunktionen. Anfragen betroffener Personen leitet er unverzüglich an den Verantwortlichen weiter.

(4) **Unterstützung nach Art. 32 bis 36 DSGVO.** Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen des Schutzes personenbezogener Daten, bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der Aufsichtsbehörde (Art. 28 Abs. 3 lit. f).

(5) **Datenschutzverletzungen.** Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens [48 Stunden — Frist festlegen] nach Bekanntwerden, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt.

(6) **Verzeichnis, Datenschutzbeauftragter.** Der Auftragsverarbeiter führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO. Datenschutzbeauftragter: [Name und Kontakt bzw. „nicht erforderlich“].

§ 4 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt eine allgemeine Genehmigung zum Einsatz der in Anhang 3 und unter https://dinetailor.com/subprocessors genannten Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO).

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens [30 — Frist festlegen] Tage vor dem Einsatz neuer oder dem Austausch bestehender Unterauftragsverarbeiter in Textform (E-Mail und Aktualisierung der Liste). Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund innerhalb von [14 — Frist festlegen] Tagen widersprechen. Können die Parteien keine Lösung finden, hat der Verantwortliche ein Sonderkündigungsrecht für den betroffenen Dienst.

(3) Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten wie in dieser Vereinbarung (Art. 28 Abs. 4 DSGVO) und haftet für deren Einhaltung.

(4) Integrationen, die der Verantwortliche selbst aktiviert und für die er einen eigenen Vertrag mit dem Anbieter hat (Anhang 3, Teil B), sind keine vom Auftragsverarbeiter eingesetzten Unterauftragsverarbeiter; der Auftragsverarbeiter stellt dort lediglich die Schnittstelle bereit. [Einordnung juristisch prüfen]

§ 5 Übermittlung in Drittländer

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten grundsätzlich in der Europäischen Union bzw. im Europäischen Wirtschaftsraum. Die Region der Datenbank ist Frankfurt am Main. Für einzelne Dienste (insbesondere KI und Telefonie) ergeben sich die Verarbeitungsregionen aus Anhang 3.

(2) Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (einschließlich EU-US Data Privacy Framework bei zertifizierten Empfängern) oder von Standardvertragsklauseln samt ergänzender Maßnahmen. Der jeweils genutzte Mechanismus steht in Anhang 3.

(3) **Ausnahme Lieferschein-Erkennung.** Die Erkennung von Lieferscheinen und Rechnungen per Foto (Wareneingang) ruft Claude Vision direkt über die Anthropic-API (USA bzw. global) auf und läuft nicht über das KI-Routing mit EU-Voreinstellung. Verarbeitet werden Bilder von Belegen der Lieferanten; Gästedaten sind dafür nicht vorgesehen. Die Übermittlung stützt sich auf die Standardvertragsklauseln des Anbieters (Anhang 3).

(4) **Telefon-KI.** Anrufer werden zu Gesprächsbeginn darauf hingewiesen, dass sie mit einer KI sprechen, und um Einwilligung zur Aufzeichnung gebeten; ohne Zustimmung werden Aufzeichnung und Transkript nicht gespeichert. Für den Telefonie-Transport ist derzeit keine EU-Region konfiguriert (Anhang 3, Twilio).

§ 6 Nachweise und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle erforderlichen Informationen zum Nachweis der Pflichten nach Art. 28 DSGVO zur Verfügung (Art. 28 Abs. 3 lit. h), etwa Prüfberichte, Zertifikate und Nachweise seiner Unterauftragsverarbeiter.

(2) Kontrollen vor Ort sind nach Vorankündigung von mindestens [14 — Frist festlegen] Tagen, während der Geschäftszeiten und ohne Störung des Betriebs zulässig, in der Regel einmal jährlich, bei konkretem Anlass auch öfter. [Kostenregelung festlegen]

§ 7 Haftung

Die Haftung richtet sich nach dem Hauptvertrag; Art. 82 DSGVO bleibt unberührt. [Haftungsregelung juristisch festlegen]

§ 8 Rückgabe und Löschung

(1) Nach Beendigung des Hauptvertrags gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten in einem gängigen, maschinenlesbaren Format heraus oder löscht sie, innerhalb von [30 — Frist festlegen] Tagen, sofern nicht eine gesetzliche Aufbewahrungspflicht entgegensteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Datensicherungen werden im regulären Zyklus überschrieben, spätestens nach [Aufbewahrungsdauer der Backups prüfen und eintragen].

(3) Gesetzliche Aufbewahrungspflichten des Verantwortlichen (z. B. § 132 BAO, § 147 AO, Aufbewahrung des Datenerfassungsprotokolls nach RKSV) bleiben unberührt; der Verantwortliche ist für die Sicherung dieser Daten vor Vertragsende selbst verantwortlich.

§ 9 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform. (2) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag geht diese Vereinbarung vor, soweit der Schutz personenbezogener Daten betroffen ist. (3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. (4) Es gilt [österreichisches / deutsches] Recht; Gerichtsstand ist [Ort].

[Ort, Datum]	[Ort, Datum]
Verantwortlicher	Auftragsverarbeiter

Anhang 1 — Gegenstand der Verarbeitung

Zwecke

Bereitstellung der Plattform: Reservierungen und Tischplanung, Gästeverwaltung (CRM), Bestellaufnahme und Kasse, Küche und Lager, Personalplanung und Zeiterfassung, Fiskal- und Buchhaltungsfunktionen, Kommunikation mit Gästen (E-Mail, Telefon), optionale KI-Funktionen.

BETROFFENE PERSONEN	DATENARTEN
Gäste und Interessenten	Name, E-Mail, Telefon, Notizen, Tags/VIP-Status, Präferenzen, Geburtstag, Besuchs- und No-Show-Historie, Reservierungen, Bestellungen und Bons, Anzahlungen, Rückmeldungen. Allergien und Unverträglichkeiten (siehe Besondere Kategorien).
Mitarbeiter des Verantwortlichen	Name, E-Mail, Telefon, Abteilung/Position, Stundensatz, Ein-/Austritt, Dienstpläne, Arbeitszeiten und Pausen, Abwesenheiten (Urlaub, Krankenstand, Sonderurlaub), Trinkgeldverteilung, Kiosk-PIN.
Bewerber	Name, Kontaktdaten, Bewerbungsunterlagen und Bewertungen (soweit das Recruiting-Modul genutzt wird).
Nutzer der Plattform (Beschäftigte des Verantwortlichen)	Name, E-Mail, Rolle, Anmeldedaten (Passwort nur als Hash), Nutzungs- und Protokolldaten.
Besteller über Lieferplattformen	Name, Telefon, E-Mail, Lieferadresse, Bestellinhalt (soweit die Lieferanbindung genutzt wird).
Anrufer	Rufnummer, Gesprächsinhalt, genannte Daten zur Reservierung, Antwort auf die Einwilligungsfrage; Aufzeichnung und Transkript nur mit Einwilligung (soweit die Telefon-KI genutzt wird).
Lieferanten (Ansprechpartner)	Name, E-Mail, Telefon, Bestell- und Rechnungsdaten.

Besondere Kategorien (Art. 9 DSGVO)

Allergien und Unverträglichkeiten im Gästeprofil sowie Krankenstände im Abwesenheitsmodul können Gesundheitsdaten sein. Ob und in welchem Umfang der Verantwortliche solche Angaben erfasst, entscheidet er selbst; er stellt die Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO (z. B. ausdrückliche Einwilligung des Gastes) sicher. [Juristisch prüfen, ob eine ergänzende Regelung nötig ist]

Anhang 2 — Technische und organisatorische Maßnahmen

Stand 21. Oktober 2026. Der Status gibt an, ob eine Maßnahme umgesetzt ist, vom Hosting-Anbieter erbracht wird (Nachweis zu hinterlegen), noch geplant ist oder in ihrer Wirksamkeit im Betrieb noch zu prüfen ist.

Vertraulichkeit (Zutritts-, Zugangs-, Zugriffs- und Trennungskontrolle)

UMGESETZT	Mandantentrennung: Daten jedes Betriebs sind durch Row-Level-Security in der Datenbank getrennt; Zugriff nur für Mitglieder des jeweiligen Betriebs.
UMGESETZT	Jede schreibende Server-Aktion im Betriebs- und Organisationsbereich prüft serverseitig die Mitgliedschaft bzw. Rolle; die Betriebs- bzw. Organisations-ID wird nie aus Client-Eingaben übernommen. Eine automatische Prüfung verhindert neue Server-Aktionen ohne Prüfung; bekannte Altfälle sind in einer Liste erfasst, die nur kleiner werden darf.
UMGESETZT	Rollen- und Berechtigungskonzept: Betriebsrollen (Mitglied, Manager) sind von Provider-Administratoren getrennt; Administrationsfunktionen sind nur für Provider-Admins erreichbar.
UMGESETZT	API-Schlüssel und Zugriffstoken (Steuerberater-Freigabe) werden nur als Hash gespeichert; der Klartext wird einmalig angezeigt.
BEIM HOSTING-ANBIETER	Transportverschlüsselung (TLS) für alle Verbindungen zur Anwendung und zur Datenbank.
BEIM HOSTING-ANBIETER	Verschlüsselung gespeicherter Daten (Datenbank, Dateispeicher, Backups).
UMGESETZT	Zugangsdaten (Schlüssel, Token, Passwörter) und erkennbare personenbezogene Angaben (E-Mail-Adressen, Telefonnummern, IBAN, Kartennummern, IP-Adressen) werden maskiert, bevor Fehler- und Störungsdaten an das Sprachmodell der Störungsanalyse, in Benachrichtigungen, Webhooks oder die GitHub-Zusammenfassung gelangen und bevor Browser-Fehlermeldungen gespeichert werden. Namen in Freitext sind nicht zuverlässig erkennbar; das Fehlerprotokoll serverseitiger Fehler bleibt dem Provider-Administrator ohne Zugangsdaten im Wortlaut sichtbar.
UMGESETZT	Datensparsame Nutzungsanalyse: eigenes, cookieloses Tracking ohne Speicherung von IP-Adressen; Einwilligungsbanner für nicht notwendige Dienste.
UMGESETZT	Datenhaltung in der EU: Datenbank in Frankfurt (eu-central-1); Serverless-Funktionen in Frankfurt (fra1). KI-Funktionen laufen standardmäßig über einen EU-Endpunkt (siehe KI-Routing unten); Ausnahmen und die Region je Dienst (KI, Telefonie) stehen in Anhang 3.
UMGESETZT	KI-Datenresidenz: In der Werkseinstellung laufen alle KI-Funktionen über einen EU-Endpunkt (Mistral); der Provider-Admin kann das ändern. Funktionen mit personenbezogenen Daten werden bei einem Nicht-EU-Endpunkt gesperrt (fail-closed), außer ein Provider-Admin setzt ein Override mit Begründung (mindestens 15 Zeichen) und Bestätigung; das Override wird im Audit-Protokoll festgehalten und im Control Center angezeigt. Ausnahme: Die Lieferschein-Erkennung ruft die direkte Anthropic-API (USA/global) auf.
UMGESETZT	Telefon-KI: Jeder Anruf beginnt mit dem Hinweis, dass der Assistent eine KI ist, gefolgt von der Einwilligungsfrage zur Aufzeichnung. Aufzeichnung und Transkript werden nur mit Zustimmung gespeichert (Prüfung in der Datenbank und Sperre im Code); die Voicemail-Aufnahme beginnt nur nach ausdrücklicher Zustimmung. Ohne klare Antwort gilt: keine Aufzeichnung.
UMGESETZT	Echtzeit-Kanäle (Reservierungen, Host-Terminal, Saalplan) werden mit dem Anmelde-Token der Sitzung autorisiert, sodass die Row-Level-Security auch für Echtzeit-Ereignisse gilt.
UMGESETZT	Zugriffe mit Service-Role-Rechten (umgehen die Row-Level-Security) sind je Datei begründet in einer Allowlist erfasst; die automatische Prüfung bricht ab, wenn ein neuer Zugriff ohne Eintrag hinzukommt. Die Inventur wird fortlaufend nachgebessert.
UMGESETZT	Die Datenbankfunktion zur Installation des Finanz-Schemas (exec_sql, DDL-fähig) ist ausschließlich für die Service-Rolle ausführbar, nicht für anonyme oder angemeldete Nutzer.
UMGESETZT	Steuerberater-Freigabe (OAuth): Der Rücksprung nach der Freigabe ist auf freigegebene Adressen beschränkt, damit ein Zugriffstoken nicht über einen manipulierten Link abfließen kann. Die Zugriffstoken sind auf Funktionsbereiche beschränkt, befristet und widerrufbar.
UMGESETZT	Zugangsdaten Dritter (API-Schlüssel der Kartenterminal-Anbieter und von fiskaly, Zugänge zu Hotel-PMS und Lieferantenportalen) werden nur verschlüsselt gespeichert (AES-256-GCM, Schlüssel in der Serverumgebung, Mandant und Verbindung gehen in die Authentisierung ein). Ohne gültigen Schlüssel wird nichts gespeichert (kein Klartext-Fallback); die Tabellen mit den Hüllen sind für Clients nicht lesbar.

UMGESETZT	Zimmerbelastung im Hotel-PMS: Aus der PMS-Antwort bleiben nur Zimmernummer, Kurzname zur Bestätigung und PMS-Referenz; Gästenamen und Kontaktdaten werden nicht gespeichert. Der gebuchte Betrag stammt aus der authentisierten Abfrage beim PMS, eine Datenbankprüfung verhindert erfundene oder nachträglich geänderte Zimmerbelastungen.
UMGESETZT	HACCP-Sensoren melden über ein eigenes Token je Sensor: nur als Hash gespeichert, zeitkonstanter Vergleich, Rate-Limit je IP und Token, Betrieb und Messstelle stammen aus dem Sensor-Eintrag, nie aus der Anfrage.
UMGESETZT	Betriebsvergleiche (Benchmarks): Teilnahme nur mit Opt-in (standardmäßig aus); Vergleichswerte nur aus Gruppen von mindestens 10 Betrieben mit komplementärer Unterdrückung, nie Einzelwerte oder Betriebs-IDs.

Integrität (Weitergabe- und Eingabekontrolle)

UMGESETZT	Eingehende Webhooks (Zahlungen, Telefonie, Lieferplattformen, Reserve with Google) werden per Signatur geprüft (zeitkonstanter Vergleich), bevor Daten verarbeitet werden.
UMGESETZT	Protokollierung administrativer Aktionen im Audit-Log (u. a. Stellvertreter-Zugriff des Supports, Kontolöschung, Feature-Flags, Nicht-EU-Overrides der KI-Anbindung); Ausbau auf alle schreibenden Betriebsaktionen ist geplant.
UMGESETZT	Stellvertreter-Zugriff durch den Support ist nur Provider-Admins möglich, wird protokolliert und im Kundenkonto durch ein Banner sichtbar gemacht.
UMGESETZT	Zahlungsereignisse von Stripe-Connect-Konten (Pay-at-Table, Anzahlung) werden nur gebucht, wenn sie vom Konto stammen, das dem Betrieb gehört; der Betrag kommt von Stripe, nicht aus Metadaten; doppelte Zahlungsereignisse für Bons werden erkannt.
UMGESETZT	Unveränderbare (append-only) Ablage der Fiskalbelege: Ändern, Löschen und Leeren der Beleg-Tabelle werden in der Datenbank verhindert (Ausnahme: Kaskade beim Löschen eines Betriebs); Korrekturen nur als neuer Beleg. Belegnummern sind je Kasse lückenlos und werden atomar in der Datenbank vergeben.
UMGESETZT	Kartenzahlungen am Terminal werden nur aus Daten gebucht, die der Anbieter auf eine authentisierte Abfrage meldet (Betrag, Trinkgeld, Status), nie aus Webhook-Inhalt oder Client-Eingaben; Webhooks ohne Signatur (SumUp) tragen ein HMAC-Token je Zahlungsversuch, ohne Konfiguration werden sie abgelehnt. Abweichende Beträge, fremde Konten oder Geräte führen zur Prüfung statt zur Buchung.

Verfügbarkeit und Belastbarkeit

BEIM HOSTING-ANBIETER	Tägliche Datensicherung der Datenbank durch den Hosting-Anbieter. Wiederherstellung zu einem beliebigen Zeitpunkt (Point-in-Time-Recovery) ist geplant; sie ist derzeit nicht aktiviert.
GEPLANT	Dokumentierter Wiederherstellungstest (Ziel: Restore in unter 2 Stunden).
GEPLANT	Öffentlicher Health-Endpoint ist vorhanden; externe Verfügbarkeitsüberwachung, öffentliche Status-Seite und Bereitschaft zu Servicezeiten sind geplant.
ZU PRÜFEN	Begrenzung der Anfragerate gegen Missbrauch. Umgesetzt mit geteiltem Zähler (Upstash Redis, EU-Region vorgesehen); ohne Konfiguration oder bei Ausfall gilt das Limit nur je Serverinstanz.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

UMGESETZT	Automatisierte Prüfungen vor jedem Zusammenführen, lokal ausgeführt (Typprüfung, Lint, Mandantentrennung, Service-Role-Allowlist, Sprach- und Textprüfungen, Unit-Tests, Mandanten-Integrationstests, Datenbank-Tests, Ende-zu-Ende-Tests). Es gibt keine unabhängige Wiederholung auf einem zweiten System.
ZU PRÜFEN	Zusammenführen von Code in den Hauptzweig nach grünem lokalem Prüflauf (pnpm gate). Es gibt keinen technischen Branch-Schutz; die Einhaltung beruht auf dem Ablauf.
GEPLANT	Externer Penetrationstest (Mandantentrennung, öffentliche Buchung, Pay-at-Table, API).
UMGESETZT	Störungs- und Sicherheitsvorfall-Prozess: Erfassung im Fehlerprotokoll, Ursachenanalyse, Meldung von Datenschutzverletzungen an den Verantwortlichen unverzüglich.

Auftragskontrolle

UMGESETZT	Unterauftragsverarbeiter werden in einer öffentlichen Liste geführt (Zweck, Datenkategorien, Region, Übermittlungsgrundlage); Änderungen werden angekündigt.
UMGESETZT	Datenexport und Kontolöschung für Nutzer der Plattform; Löschung bzw. Rückgabe von Betriebsdaten nach Vertragsende auf Weisung des Verantwortlichen.
UMGESETZT	Besonders sensible Funktionen werden nur vom Provider-Admin freigeschaltet: die scharfe Fiskalisierung (Flag fiscal_at_ga) und die eingefrorenen Module (Flag labs). Betriebe können die Flags lesen, aber nicht setzen; jede Änderung wird protokolliert.
UMGESETZT	Buchung über KI-Assistenten: nur für Betriebe mit ausdrücklichem Opt-in sichtbar (standardmäßig aus); die Schnittstelle arbeitet über einen anonymen RPC-Zugang statt mit Service-Rolle, mit Ratenbegrenzung, und speichert die Einwilligung des Gastes mit Version der Bedingungen.
UMGESETZT	Lohn-Exporte (z. B. für Crésus oder Swissdec-zertifizierte Lohnprogramme) sind reine Dateien zum Download; DineTailor übermittelt keine Lohndaten an Dritte.

Anhang 3 — Unterauftragsverarbeiter

Quelle: https://dinetailor.com/subprocessors · Stand 21. Oktober 2026. Die laufend gepflegte Liste ist maßgeblich.

KI-Routing und Datenresidenz

- Standard: Alle 56 KI-Funktionen sind ab Werk an Mistral Large 3 über den EU-Endpunkt api.eu.mistral.ai gebunden.
- 24 dieser Funktionen verarbeiten personenbezogene Daten (Gäste, Mitarbeiter, Bewerber, Konten); die übrigen arbeiten nach der Klassifikation im Code ohne Personenbezug.
- Der Plattform-Betreiber (Provider-Admin) kann den Standard und einzelne Funktionen auf andere Anbieter umstellen, auch auf Anbieter außerhalb der EU. Funktionen mit personenbezogenen Daten werden bei einem Nicht-EU-Endpunkt gesperrt, solange kein Override vorliegt (fail-closed). Ein Override verlangt eine Begründung von mindestens 15 Zeichen und eine ausdrückliche Bestätigung, wird im Audit-Protokoll festgehalten und ist im Control Center sichtbar.
- Ausnahme: Die Lieferschein-Erkennung (Foto-Wareneingang) ruft Claude Vision fest über api.anthropic.com (USA bzw. global) auf und läuft nicht über dieses Routing. Verarbeitet werden Bilder von Lieferscheinen und Rechnungen der Lieferanten (keine Gästedaten vorgesehen).
- Information der Verantwortlichen über Nicht-EU-Overrides: [Frist und Verfahren festlegen]

Teil A — Unterauftragsverarbeiter

Supabase · Supabase Inc. (USA) — Vertragsrechtsträger laut Vertrag zu prüfen · Aktiv

Zweck	Datenbank (Postgres), Authentifizierung, Dateispeicher (Logos, Belege) und Echtzeit-Synchronisation für alle Module.
Datenkategorien	Stammdaten der Betriebe; Gästedaten (Name, E-Mail, Telefon, Notizen, Allergien, Präferenzen, Geburtstag); Reservierungen und Bestellungen/Bons; Mitarbeiterdaten (Stammdaten, Arbeitszeiten, Stundensatz); Fiskal- und Finanzdaten; Zugangsdaten (E-Mail, Passwort-Hash); Hochgeladene Dateien
Region	**EU/EWR** — EU — Frankfurt (AWS eu-central-1), Projekt „dinetailor“ (Projektregion per Supabase CLI am 20.10.2026 ausgelesen).
Übermittlung	**Standardvertragsklauseln (SCC)** — Supabase-DPA (Version 1, 01.08.2026): EU-Standardvertragsklauseln (Beschluss 2021/914), UK-Addendum, Schweizer Zusatz. Data Privacy Framework wird im DPA nicht erwähnt.

Vercel · Vercel Inc. (USA) · Aktiv

Zweck	Hosting der Web-Anwendung, Ausführung der Serverless-Funktionen und Cron-Jobs, Auslieferung über ein CDN.
Datenkategorien	Verbindungsdaten (IP-Adresse, User-Agent, Header); Request-/Response-Inhalte während der Verarbeitung; Laufzeit-Logs
Region	**Teilweise EU/EWR** — Funktionen: Frankfurt (fra1, per vercel.json). Auslieferung, Logs und Verwaltungsdaten können außerhalb der EU liegen.
Übermittlung	**Standardvertragsklauseln (SCC)** — Vercel-DPA (Stand 31.03.2026): EU-Standardvertragsklauseln 2021 und UK-IDTA. Das Data Privacy Framework wird im DPA nicht erwähnt.

Stripe · Stripe-Rechtsträger laut Vertrag zu prüfen (das DPA verweist auf die „in der Vereinbarung angegebene Stripe-Rechtsperson“) · Aktiv

Zweck	Zahlungsabwicklung: Abonnements der Betriebe, Anzahlungen (Deposits), Gutscheine, Zahlung am Tisch (auch TWINT in der Schweiz) und Shop-Zahlungen für Online-Bestellungen über Stripe Connect (Express, Direct Charges). Zusätzlich Kartenzahlung am Terminal (Stripe Terminal, serverseitig gesteuert): Zahlungsauftrag an das Lesegerät, Gerätekopplung, Ergebnis-Abfrage.
Datenkategorien	Name, E-Mail, Rechnungsdaten; Zahlungsdaten (Karte/SEPA/TWINT — werden direkt an Stripe übertragen und nicht bei DineTailor gespeichert; bei Stripe Terminal läuft die Karte nur zwischen Lesegerät und Stripe); Beträge, Währung, Zahlungsstatus, am Terminal gewähltes Trinkgeld; Beschreibung „DineTailor Bon #<Nr>“ und eine interne Zahlungs-ID (Metadaten) je Terminalzahlung; Shop-Zahlung (Direct Charge auf dem Stripe-Konto des Betriebs): Positionsbezeichnungen und Beträge der Bestellung, Beschreibung „Online-Bestellung <Abholcode> · <Betrieb>“, optional die E-Mail-Adresse des Gastes (Checkout-Vorbelegung); in den Metadaten nur die Bestell-ID, keine weiteren Kundendaten; Terminal-Gerätedaten: Registrierungscode, Gerätename, Standort; Betriebsdaten für das Stripe-Onboarding (Connect)
Region	**Zu prüfen** — EU/USA — Verarbeitungsorte laut Stripe-Vertrag und Stripe-Subprozessorliste zu prüfen.
Übermittlung	**Data Privacy Framework und Standardvertragsklauseln** — Stripe-DPA, Abschn. 8: EU-US Data Privacy Framework, EU-Standardvertragsklauseln (Module 1, 2, ggf. 3) und UK-Addendum.

Mistral AI · Mistral AI (Frankreich) — Vertragsrechtsträger zu prüfen · Aktiv

Zweck	Textgenerierung und -analyse für alle KI-Funktionen der Plattform (Concierge-Chat, Menü-/Weinassistenten, Prognosen, Dienstplan-Vorschläge, Telefon-Assistent u. a.).
Datenkategorien	Prompt-Inhalte je Funktion — überwiegend Speisekarte, Rezepte, Kennzahlen; Bei Funktionen mit Personenbezug: Gastname, Telefon/E-Mail, Reservierungsnotizen, Allergien, Gast-Historie, Gesprächsinhalte (Chat, Telefon), Mitarbeiter- und Bewerberdaten, Konto-Daten (siehe KI-Routing)
Region	**EU/EWR** — EU — regionaler Endpunkt api.eu.mistral.ai (per Umgebungsvariable MISTRAL_BASE_URL änderbar). Bei geändertem Endpunkt klassifiziert die Plattform die Region neu; ein unbekannter Host zählt als Nicht-EU.
Übermittlung	**Zu prüfen** — EU-Unternehmen mit EU-Endpunkt; DPA und Subprozessorliste von Mistral (u. a. eingesetzter Cloud-Anbieter) noch nicht geprüft.

AWS (Amazon Bedrock) — Claude · Amazon Web Services (Rechtsträger laut Vertrag zu prüfen; US-Konzern) · Optional (nur bei Aktivierung)

Zweck	Claude-Modelle (Anthropic) über AWS Bedrock mit EU-Geo-Inferenzprofil, als EU-Alternative zur direkten Anthropic-API.
Datenkategorien	Prompt-Inhalte je Funktion (siehe Mistral); Bei Funktionen mit Personenbezug: dieselben Datenklassen wie bei Mistral
Region	**EU/EWR** — EU — Region aus der Umgebungsvariable BEDROCK_REGION (Standard eu-central-1, Frankfurt), Modell nur mit EU-Geo-Inferenzprofil (Modell-ID eu.*). Das Profil verteilt die Verarbeitung auf EU-Regionen.
Übermittlung	**Zu prüfen** — AWS-Vertragswerk (DPA, Standardvertragsklauseln, DPF-Status) und Verfügbarkeit der gewünschten Claude-Modelle im EU-Profil noch nicht geprüft.

Anthropic (Claude, direkte API) · Anthropic PBC (USA) — Vertragsrechtsträger zu prüfen · Optional (nur bei Aktivierung)

Zweck	(a) Bildanalyse von Lieferscheinen und Rechnungen (Claude Vision). (b) Textgenerierung nur bei ausdrücklicher Bindung durch den Provider-Admin.
Datenkategorien	(a) Bilder von Lieferscheinen und Rechnungen: Lieferant, Positionen, Mengen, Preise, Rechnungsdaten — keine Gästedaten vorgesehen; (b) Prompt-Inhalte der gebundenen Funktionen (siehe Mistral)
Region	**Außerhalb EU/EWR** — USA bzw. global — die direkte Claude-API bietet laut Doku nur die Inferenzregionen „us“ und „global“ und keinen EU-Endpunkt. Endpunkt: api.anthropic.com.
Übermittlung	**Standardvertragsklauseln (SCC)** — Anthropic-DPA: EU-Standardvertragsklauseln (Modul 2/3). Eine Zertifizierung unter dem Data Privacy Framework ist nicht belegt (zu prüfen).

OpenAI · OpenAI (Rechtsträger laut Vertrag zu prüfen; US-Konzern) · Optional (nur bei Aktivierung)

Zweck	Textgenerierung und -analyse für KI-Funktionen (alternativer Anbieter).
Datenkategorien	Prompt-Inhalte je Funktion (siehe Mistral); Bei Funktionen mit Personenbezug: dieselben Datenklassen wie bei Mistral
Region	**Zu prüfen** — Konfigurierter Endpunkt: eu.api.openai.com (per OPENAI_BASE_URL änderbar). EU-Residenz gilt nur mit einem Schlüssel aus einem OpenAI-Projekt mit Region Europa.
Übermittlung	**Zu prüfen** — Transfermechanismus laut OpenAI-DPA noch nicht geprüft.

Google Gemini · Google (Rechtsträger laut Vertrag zu prüfen; US-Konzern) · Optional (nur bei Aktivierung)

Zweck	Textgenerierung und -analyse für KI-Funktionen (alternativer Anbieter).
Datenkategorien	Prompt-Inhalte je Funktion (siehe Mistral); Bei Funktionen mit Personenbezug: dieselben Datenklassen wie bei Mistral
Region	**Zu prüfen** — Konfigurierter Endpunkt: generativelanguage.googleapis.com — ohne Regionszusage, Verarbeitungsort nicht belegt. EU-Residenz gäbe es nur über Vertex AI; diese Anbindung besteht nicht.
Übermittlung	**Zu prüfen** — Transfermechanismus laut Google-Vertragswerk noch nicht geprüft.

Twilio · Twilio Inc. (USA) · Optional (nur bei Aktivierung)

Zweck	Rufnummern und Telefonie für den Telefon-Assistenten: Annahme der Anrufe, KI-Hinweis und Einwilligungsabfrage zur Aufzeichnung (Sprache oder Taste), Sprachausgabe der Ansagen, Weiterleitung, Voicemail nur mit Zustimmung; später Audio-Streaming (Media Streams).
Datenkategorien	Rufnummer des Anrufers und des Betriebs; Gesprächsaudio (Stimme, genannte Namen und Daten); Antwort auf die Einwilligungsfrage (Taste oder gesprochenes Ja/Nein, von Twilios Spracherkennung <Gather> ausgewertet); Voicemail-Aufnahmen — nur nach ausdrücklicher Zustimmung; Verbindungsdaten (Zeitpunkt, Dauer); Ansagetexte (Sprachausgabe: deutsche Ansagen mit einer Amazon-Polly-Stimme, andere Sprachen mit Twilios Standardstimme)
Region	**Außerhalb EU/EWR** — Standardregion US1 (USA). Twilio bietet die Region Irland (IE1); Media Streams sind dort seit 23.04.2024 verfügbar. Konfiguriert ist derzeit keine Region.
Übermittlung	**Data Privacy Framework und Standardvertragsklauseln** — Twilio-DPA (Schedule 3, Stand 09.04.2026): Twilio Inc. ist unter dem EU-US Data Privacy Framework selbstzertifiziert; weitere Mechanismen: Binding Corporate Rules, EU-Standardvertragsklauseln.

Deepgram · Deepgram (Rechtsträger laut Vertrag zu prüfen) · Geplant (noch nicht im Einsatz)

Zweck	Sprache-zu-Text (Live-Transkription) der Telefongespräche.
Datenkategorien	Gesprächsaudio (Stimme, genannte Namen, Telefonnummern, Wünsche); Transkripte
Region	**Zu prüfen** — Standard: api.deepgram.com (nicht auf die EU beschränkt). Verfügbar: EU-Endpunkt api.eu.deepgram.com (laut Deepgram seit Dezember 2025 allgemein verfügbar).
Übermittlung	**Zu prüfen** — Die Deepgram-Trust-Seite nennt weder DPF noch SCC; DPA und Mechanismus sind mit Deepgram zu klären.

ElevenLabs · ElevenLabs (Rechtsträger laut Vertrag zu prüfen) · Geplant (noch nicht im Einsatz)

Zweck	Text-zu-Sprache (Stimme des Telefon-Assistenten).
Datenkategorien	Antworttexte des Assistenten (können Namen, Uhrzeiten, Personenzahl enthalten)
Region	**Außerhalb EU/EWR** — Standard: USA. EU-Datenresidenz nur für Enterprise-Kunden über eine isolierte Umgebung (api.eu.residency.elevenlabs.io), mit separatem Konto und Schlüssel.
Übermittlung	**Zu prüfen** — DPA mit Standardvertragsklauseln und DPF-Status nur aus Sekundärquellen bekannt; vor Einsatz am Originaldokument bzw. im DPF-Register zu prüfen.

Resend · Resend Inc. (USA) · Optional (nur bei Aktivierung)

Zweck	Versand von Transaktions-E-Mails: Buchungsbestätigungen und -erinnerungen, Einladungen von Teammitgliedern, Rechnungen (E-Rechnung) an Geschäftskunden, Bestellungen an Lieferanten, Monatsberichte (ROI) und Betriebsbenachrichtigungen an die Betreiber.
Datenkategorien	E-Mail-Adresse und Name des Empfängers; E-Mail-Inhalt (Reservierungsdetails: Datum, Uhrzeit, Personenzahl, Betrieb; Kennzahlen im Monatsbericht); Anhänge: E-Rechnung (XML und PDF) an Geschäftskunden, Bestellung (PDF, CSV oder EDIFACT) an Lieferanten; Zustellprotokolle
Region	**Außerhalb EU/EWR** — USA — laut Resend-DPA (Abschn. 6.1) finden die primären Verarbeitungsvorgänge in den USA statt. Eine EU-Region ist nicht belegt.
Übermittlung	**Data Privacy Framework und Standardvertragsklauseln** — Resend-DPA (Stand 31.12.2025): EU-Standardvertragsklauseln (Abschn. 6.2) sowie Selbstzertifizierung unter EU-US Data Privacy Framework (Abschn. 11.1).

SMTP-Relay (vom Plattform-Betreiber konfiguriert) · Anbieter noch festzulegen (Konfiguration im Control Center, Tabelle smtp_config) · Optional (nur bei Aktivierung)

Zweck	Versand von Plattform-Mails (Benachrichtigungen, Feedback-Antworten, Admin-Mails) über einen frei konfigurierbaren SMTP-Server.
Datenkategorien	E-Mail-Adresse und Name des Empfängers; E-Mail-Inhalt
Region	**Zu prüfen** — Abhängig vom gewählten SMTP-Anbieter — zu prüfen, sobald der Anbieter feststeht.
Übermittlung	**Zu prüfen** — Anbieter nicht festgelegt; Transfermechanismus nach Auswahl zu prüfen.

Upstash (Redis) · Upstash Inc. (USA) — Rechtsträger zu prüfen · Optional (nur bei Aktivierung)

Zweck	Verteiltes Rate-Limiting (Schutz vor Missbrauch und Massenbuchungen) über einen gemeinsamen Zähler.
Datenkategorien	IP-Adresse des Besuchers als Teil des Zähler-Schlüssels (Form rl:<nav|action>:<IP>:<Zeitfenster>); Zählerstand je Zeitfenster; keine weiteren Inhalte
Region	**Zu prüfen** — Wird beim Anlegen der Datenbank gewählt; vorgesehen ist eine einzelne EU-Region. Konkrete Region und Replikation sind noch festzulegen.
Übermittlung	**Zu prüfen** — Das DPA von Upstash wurde nicht im Volltext geprüft; DPF-Selbstzertifizierung und Europa-Anhang sind vor Einsatz am Originaldokument zu bestätigen.

fiskaly (SIGN AT, SIGN DE, DSFinV-K) · fiskaly (Rechtsträger und Sitz laut Vertrag zu prüfen) · Optional (nur bei Aktivierung)

Zweck	AT: Cloud-Signatur der Belege nach Registrierkassensicherheitsverordnung (RKSV), Belegketten, DEP-Export. DE: Sicherung der Vorgänge in der zertifizierten Cloud-TSE (fiskaly SIGN DE: Start- und Abschluss-Transaktionen für Bestellungen und Belege nach KassenSichV), Übermittlung des Kassenabschlusses (DSFinV-K, Cash Point Closing) und Abruf des Datenexports für die Finanzverwaltung.
Datenkategorien	AT: Belegdaten (Positionen, Beträge, Steuersätze, Zahlart, Zeitpunkt, Kassen-ID); DE (TSE): Transaktionsdaten je Bestellung/Beleg (Positionen, Beträge je Steuersatz, Zahlart Bar/Unbar, Zeitpunkte, Kassen-/Client-ID; keine Gästedaten), TSS-/Client-Kennungen; PUK und Admin-PIN werden nicht gespeichert; DE: Kassenabschluss — Bons mit Positionen (Bezeichnung, Menge, Preis, Steuersatz), Zahlarten und Beträge, Storno/Training, Kassen-ID, Bediener (Kennung und Name, höchstens 50 Zeichen); Zugangsdaten des Betriebs bei fiskaly (API-Schlüssel; in der Konfiguration des Betriebs gespeichert, Zugriff nur über Rollenrechte)
Region	**Zu prüfen** — Rechenzentrumsstandort laut fiskaly-Vertrag zu prüfen (nicht belegt).
Übermittlung	**Zu prüfen** — AVV und Verarbeitungsorte von fiskaly noch nicht geprüft.

GitHub · GitHub Inc. (USA, Microsoft-Konzern) — Rechtsträger zu prüfen · Optional (nur bei Aktivierung)

Zweck	Lesen von Quellcode für die KI-gestützte Störungsanalyse, Anlegen von Entwurfs-Pull-Requests, Bereitstellung privater Pakete.
Datenkategorien	Quellcode-Auszüge und Pull-Request-Texte; Gegebenenfalls Fehlermeldungen und Stack-Traces in Beschreibungstexten
Region	**Zu prüfen** — Zu prüfen (GitHub-Subprozessorliste).
Übermittlung	**Zu prüfen** — GitHub-Datenschutzvereinbarung noch nicht geprüft.

Teil B — Vom Verantwortlichen aktivierte Integrationen und eigenverantwortliche Dritte

SumUp (Kartenterminal, empfohlen) · SumUp Limited (Dublin, Irland), SumUp Payments Limited (London, Vereinigtes Königreich) oder SumUp EU Payments, UAB (Vilnius, Litauen) — je nach Vertrag des Betriebs; für Österreich/Deutschland nennt SumUp keine feste Gesellschaft · Optional (nur bei Aktivierung)

Zweck	Kartenzahlung am SumUp-Solo-Terminal über die Cloud-API: Zahlungsauftrag an das Gerät, Gerätekopplung, Abfrage des Zahlungsergebnisses inklusive Trinkgeld; Abgleich der gebuchten Zahlung mit der Bon-Summe.
Datenkategorien	An SumUp gesendet: Betrag, Währung, Bezeichnung „DineTailor Bon #<Nr>“ (höchstens 200 Zeichen), Rücksprung-Adresse (return_url mit Prüfwert), Trinkgeld-Stufen und -Zeitlimit, Kopplungscode und Gerätename, interne Zahlungs-ID als Fremd-Transaktions-ID; Zugangsdaten: API-Schlüssel und Händlercode des Betriebs (bei DineTailor verschlüsselt gespeichert) sowie der Affiliate-Schlüssel der Plattform; Von SumUp empfangen: Zahlungsstatus, Gesamtbetrag und Trinkgeld, Währung, Transaktionskennung, Händlercode; Keine Kartendaten bei DineTailor (die Karte läuft nur zwischen Gerät und SumUp)
Region	**Teilweise EU/EWR** — Laut Datenschutzerklärung von SumUp (Stand 27.03.2025) werden personenbezogene Daten des Europageschäfts im Europäischen Wirtschaftsraum gespeichert; Übermittlungen an Gruppengesellschaften und Dritte außerhalb von EWR/UK sind möglich.
Übermittlung	**Zu prüfen** — SumUp nennt für Übermittlungen außerhalb von EWR/UK „vertragliche Vereinbarungen“ und ein „angemessenes Datenschutzniveau“, aber weder Standardvertragsklauseln noch einen Angemessenheitsbeschluss ausdrücklich. Vertrag zwischen DineTailor und SumUp (Partnerprogramm, Affiliate-Schlüssel) noch nicht geprüft.

TWINT (Zahlung in der Schweiz) · TWINT AG, Stauffacherstrasse 41, 8004 Zürich (Schweiz) · Optional (nur bei Aktivierung)

Zweck	Zahlungsmittel-Betreiber: Der Gast bestätigt die Zahlung in der TWINT-App; TWINT meldet Erfolg oder Fehlschlag über Stripe zurück.
Datenkategorien	Betrag und Währung (CHF) der Zahlung; Name des Betriebs (Name des verbundenen Stripe-Kontos, wird dem Gast in der TWINT-App angezeigt); Onboarding-Angaben des Betriebs, die Stripe für die Prüfung durch TWINT verlangt (Firma, Anschrift, Kontakt, Website); Keine Gästedaten, die DineTailor selbst an TWINT sendet; die Daten des Gastes liegen bei TWINT und seiner Bank
Region	**Teilweise EU/EWR** — Schweiz. Laut Datenschutzerklärung der TWINT AG (Stand August 2026) liegen Daten auf Servern in der Schweiz oder in der EU; die Bearbeitung kann auch im Ausland erfolgen, vor allem in Deutschland und den USA.
Übermittlung	**Zu prüfen** — Die Übermittlung an TWINT in der Schweiz erfolgt durch Stripe als Auftragsverarbeiter. Welche Grundlage dafür gilt (z. B. Angemessenheitsbeschluss für die Schweiz), ist zu prüfen. TWINT nennt für eigene Übermittlungen in Länder ohne angemessenen Schutz Standardvertragsklauseln.

ready2order · ready2order (Rechtsträger und Sitz zu prüfen) · Optional (nur bei Aktivierung)

Zweck	Abruf von Rechnungen und Umsätzen der bestehenden Kasse des Betriebs für Auswertungen (z. B. Prime Cost).
Datenkategorien	Belegdaten (Positionen, Beträge, Zeitpunkt)
Region	**Zu prüfen** — Laut Vertrag des Betriebs mit dem Anbieter zu prüfen.
Übermittlung	**Zu prüfen** — Vertragsverhältnis liegt beim Betrieb; Einordnung zu prüfen.

HelloCash · HelloCash (Rechtsträger und Sitz zu prüfen) · Optional (nur bei Aktivierung)

Zweck	Abruf von Rechnungen und Umsätzen der bestehenden Kasse des Betriebs für Auswertungen.
Datenkategorien	Belegdaten (Positionen, Beträge, Zeitpunkt)
Region	**Zu prüfen** — Laut Vertrag des Betriebs mit dem Anbieter zu prüfen.
Übermittlung	**Zu prüfen** — Vertragsverhältnis liegt beim Betrieb; Einordnung zu prüfen.

orderbird · orderbird (Rechtsträger und Sitz zu prüfen) · Optional (nur bei Aktivierung)

Zweck	Abruf von Rechnungen und Umsätzen der bestehenden Kasse des Betriebs für Auswertungen.
Datenkategorien	Belegdaten (Positionen, Beträge, Zeitpunkt)
Region	**Zu prüfen** — Laut Vertrag des Betriebs mit dem Anbieter zu prüfen.
Übermittlung	**Zu prüfen** — Vertragsverhältnis liegt beim Betrieb; Einordnung zu prüfen.

Lieferando · Betreiber der Lieferplattform (Rechtsträger und Sitz zu prüfen) · Optional (nur bei Aktivierung)

Zweck	Empfang von Lieferbestellungen (Webhook) zur Anzeige in Küche und Auswertung.
Datenkategorien	Name, Telefon, E-Mail und Lieferadresse des Bestellers; Bestellpositionen, Beträge, Lieferzeit
Region	**Zu prüfen** — Laut Vertrag des Betriebs mit der Plattform zu prüfen.
Übermittlung	**Zu prüfen** — Daten fließen von der Plattform zu DineTailor (eingehend); Vertragsverhältnis liegt beim Betrieb.

Wolt · Betreiber der Lieferplattform (Rechtsträger und Sitz zu prüfen) · Optional (nur bei Aktivierung)

Zweck	Empfang von Lieferbestellungen (Webhook) zur Anzeige in Küche und Auswertung.
Datenkategorien	Name, Telefon, E-Mail und Lieferadresse des Bestellers; Bestellpositionen, Beträge, Lieferzeit
Region	**Zu prüfen** — Laut Vertrag des Betriebs mit der Plattform zu prüfen.
Übermittlung	**Zu prüfen** — Daten fließen von der Plattform zu DineTailor (eingehend); Vertragsverhältnis liegt beim Betrieb.

Uber Eats · Betreiber der Lieferplattform (Rechtsträger und Sitz zu prüfen) · Optional (nur bei Aktivierung)

Zweck	Empfang von Lieferbestellungen (Webhook) zur Anzeige in Küche und Auswertung.
Datenkategorien	Name, Telefon, E-Mail und Lieferadresse des Bestellers; Bestellpositionen, Beträge, Lieferzeit
Region	**Zu prüfen** — Laut Vertrag des Betriebs mit der Plattform zu prüfen.
Übermittlung	**Zu prüfen** — Daten fließen von der Plattform zu DineTailor (eingehend); Vertragsverhältnis liegt beim Betrieb.

Reserve with Google · Google (Rechtsträger zu prüfen) · Geplant (noch nicht im Einsatz)

Zweck	Buchbarkeit von Restaurants in Google Suche und Maps: Bereitstellung von Betriebsstammdaten und Verfügbarkeit, Entgegennahme von Buchungen.
Datenkategorien	Betriebsstammdaten (Name, Adresse, Telefon, Geokoordinaten, Küche); Verfügbarkeiten; Buchungsdaten des Gastes (Name, Kontaktdaten, Personenzahl, Zeitpunkt)
Region	**Zu prüfen** — Globale Google-Infrastruktur — Verarbeitungsorte zu prüfen.
Übermittlung	**Zu prüfen** — Konditionen des Google-Partnervertrags noch nicht geprüft.

TaxTailor (Steuerberater-Schnittstelle) · TaxTailor — Rechtsträger zu prüfen (Schwesterprodukt, Pakete @clouddnagmbh) · Optional (nur bei Aktivierung)

Zweck	Bereitstellung von Buchungsjournal, Kontenplan und Mandantenstammdaten für den Steuerberater bzw. dessen Buchhaltungssystem. Die Daten werden von dort mit einem Zugriffstoken abgerufen (Pull-Schnittstelle).
Datenkategorien	Buchungsjournal (Beträge, Konten, Belegreferenzen); Kontenplan; Mandantenstammdaten (Betrieb)
Region	**Zu prüfen** — Zu prüfen. Beobachtung: Das zugehörige Supabase-Projekt „taxtailor“ liegt laut Supabase CLI (20.10.2026) in eu-west-2 (London, UK).
Übermittlung	**Zu prüfen** — Vertragsverhältnis Betrieb ↔ Steuerberater ↔ TaxTailor und Angemessenheit der Region (UK) zu prüfen.

Apaleo (Hotel-PMS) · Apaleo (Rechtsträger und Sitz zu prüfen) — laut Subunternehmerliste (Stand 10.10.2022) Infrastruktur bei Amazon Web Services EMEA SARL · Optional (nur bei Aktivierung)

Zweck	Zimmerbelastung: Hausgast anhand von Zimmernummer und Nachname verifizieren, den Bon-Betrag je Steuersatz als Belastung auf das Gästefolio buchen, das Ergebnis nachlesen und bei Fehlern ausgleichen.
Datenkategorien	An Apaleo gesendet: Zimmernummer (Suche nach Hausgästen), Property-, Reservierungs- und Folio-Kennung; je Belastung Betrag, Währung, Steuertyp, Bezeichnung „<Betrieb> · Bon <Nr>“ (höchstens 120 Zeichen) und die Versuchs-ID (Beleg- und Idempotenzschlüssel); Zugangsdaten des Hotels (Client-ID, Client-Secret; bei DineTailor verschlüsselt gespeichert); Von Apaleo empfangen und bis auf Zimmernummer, Kurzname (Initial und Nachname, zur Bestätigung) und Referenz sofort verworfen: Reservierungs- und Gästedaten; gespeichert werden nur Zimmernummer und Referenzen, keine Namen oder Kontaktdaten
Region	**Zu prüfen** — Laut Subunternehmerliste von Apaleo läuft die Anwendung auf AWS (Amazon Web Services EMEA SARL, DE); die AWS-Region ist nicht genannt. Die Liste ist auf den 10.10.2022 datiert und nennt auch US-Unterauftragnehmer (u. a. für Monitoring und Support).
Übermittlung	**Zu prüfen** — Die Subunternehmerliste nennt keinen Übermittlungsmechanismus. Vertragsverhältnis liegt beim Hotel (Apaleo ↔ Hotel); ein AVV zwischen DineTailor und Apaleo besteht nicht und ist für diese Anbindung auch nicht belegt.

Mews (Hotel-PMS) · Mews — Rechtsträger laut Vertrag des Hotels (laut Mews-DPA gilt das im Vertrag genannte Mews-Affiliate) · Optional (nur bei Aktivierung)

Zweck	Zimmerbelastung: Hausgast über Zimmernummer finden und mit dem Nachnamen verifizieren, den Bon-Betrag als Posten auf das Gästeprofil buchen (Add order), Ergebnis nachlesen, bei Bedarf stornieren.
Datenkategorien	An Mews gesendet: Zimmerbezeichnung (Suche), Gast-/Reservierungskennungen; je Belastung Betrag, Währung, Steuercode, Bezeichnung „DineTailor <Betrieb> · Bon <Nr> · <Versuchs-ID>“ (höchstens 250 Zeichen), Reservierungs-ID und Versuchs-ID als externe Kennung; in jedem Aufruf ClientToken, AccessToken und Client-Name; Zugangsdaten des Hotels (AccessToken; bei DineTailor verschlüsselt gespeichert) und der Plattform (ClientToken); Von Mews empfangen und bis auf Zimmernummer, Kurzname (Initial und Nachname) und Referenz sofort verworfen: Kunden- und Reservierungsdaten; gespeichert werden nur Zimmernummer und Referenzen
Region	**Zu prüfen** — Laut Mews werden Daten je nach Mews-Produkt und Konfiguration des Kunden in der Europäischen Union oder in den USA gehostet. Die Region des einzelnen Hotels ist beim Hotel bzw. bei Mews zu erfragen.
Übermittlung	**Standardvertragsklauseln (SCC)** — Mews-DPA (Version 3.4, 30.03.2026): Übermittlungen in Drittländer über Angemessenheitsbeschluss, Art.-46-Garantien oder Ausnahmen; als Garantie sind die Standardvertragsklauseln (Beschluss 2021/914, Module 2 und 3) eingebunden, dazu UK- und Schweiz-Addendum. Das Data Privacy Framework wird nicht erwähnt. Das DPA regelt das Verhältnis Hotel ↔ Mews, nicht das zu DineTailor.

Großhändler und Lieferanten (Bestell- und EDI-Postfächer) · Lieferanten des Betriebs, z. B. Transgourmet, METRO, Selgros, Kastner und deren EDI-Dienstleister — je nach Vertrag des Betriebs; Rechtsträger zu prüfen · Optional (nur bei Aktivierung)

Zweck	Empfang der vom Betrieb freigegebenen Sammelbestellungen als PDF und CSV oder als EDIFACT-ORDERS-Datei im Anhang.
Datenkategorien	Bestellpositionen (Artikel, Mengen, Gebinde, Preise, Summen) und Lieferdatum; Standortname, Kundennummer je Standort, GLN von Besteller und Lieferstelle; Ansprechpartner des Betriebs (Name, E-Mail, Telefon), Vertragsreferenz und Bemerkungen; Keine Gästedaten
Region	**Zu prüfen** — Beim jeweiligen Lieferanten bzw. dessen EDI-Dienstleister; liegt im Vertragsverhältnis des Betriebs und ist dort zu prüfen.
Übermittlung	**Zu prüfen** — Der Betrieb sendet Bestellungen an seinen eigenen Lieferanten. Ob der Lieferant selbstständig Verantwortlicher oder Auftragsverarbeiter ist, und die Standorte seiner Postfächer, sind nicht geprüft.

KI-Assistenten (MCP-Schnittstelle, eingehend) · Betreiber der KI-Assistenten, über die Gäste Reservierungen anfragen (z. B. ChatGPT, Claude) — Rechtsträger zu prüfen · Optional (nur bei Aktivierung)

Zweck	Gäste finden über einen KI-Assistenten freie Tische und senden Reservierungsanfragen an freigeschaltete Betriebe.
Datenkategorien	Vom Assistenten an DineTailor: Vor- und Nachname, E-Mail, Telefonnummer des Gastes, Gruppengröße, Wunschzeit, Einwilligung zur Datenverarbeitung; Von DineTailor an den Assistenten: öffentliche Betriebsdaten, freie Zeiten, Bestätigungs-Token der Anfrage; Keine Zahlungsdaten
Region	**Zu prüfen** — Beim jeweiligen Assistenten-Anbieter; DineTailor hat darauf keinen Einfluss. Die Eingaben des Gastes verarbeitet der Anbieter des Assistenten unter eigener Verantwortung.
Übermittlung	**Zu prüfen** — Die Daten fließen vom Gast über seinen Assistenten zu DineTailor; ob und wohin der Assistenten-Anbieter sie übermittelt, liegt außerhalb von DineTailor.

Browser-Spracherkennung (Web Speech API) · Browser-Hersteller des jeweiligen Endgeräts (z. B. Google für Chrome, Apple für Safari) · Optional (nur bei Aktivierung)

Zweck	Umwandlung gesprochener Befehle (z. B. „Tisch 4 platzieren“, Bestellungen) in Text im Browser des Mitarbeiters.
Datenkategorien	Gesprochene Anweisungen des Mitarbeiters (Audio)
Region	**Zu prüfen** — Liegt beim Browser-Hersteller; je nach Browser kann das Audio an dessen Server übertragen werden. Nicht von DineTailor beauftragt oder kontrollierbar.
Übermittlung	**Zu prüfen** — Abhängig vom Browser-Hersteller; nicht von DineTailor vertraglich geregelt.