

GALLESIS · DOKUMENT 03

Auftragsbearbeitungsvertrag mit den Anlagen A–E

Zu unterzeichnen — zwei Parteien

Fassung	1.2 vom 11. Oktober 2026
Unterzeichnung	Der Kunde als Verantwortlicher und Gallesis als Auftragsbearbeiterin.
Einsatz	Mit jedem Kunden, bevor die ersten Personendaten bearbeitet werden.
Sprache	Deutsch (Schweiz). Massgebend ist diese Fassung.

zwischen

[KUNDE-FIRMA], [KUNDE-ADRESSE], UID [KUNDE-UID]

— nachfolgend «Verantwortlicher» —

und

Gallesis (Einzelunternehmen; Inhaber gemäss Impressum auf gallesis.com), Bireggstrasse 1, 6003 Luzern

— nachfolgend «Auftragsbearbeiterin» oder «Gallesis» —

Präambel

Der Verantwortliche nutzt die Software Gallesis für den Betrieb seines Unternehmens. Gallesis bearbeitet dabei Personendaten im Auftrag und nach Weisung des Verantwortlichen. Dieser Vertrag regelt diese Bearbeitung nach Art. 9 DSGVO. Er ist integrierender Bestandteil des Hauptvertrags (AGB und Abonnementbedingungen). Unterliegt der Verantwortliche zusätzlich der DSGVO, gilt dieser Vertrag zugleich als Vertrag nach Art. 28 Abs. 3 DSGVO.

1. Begriffe

1.1 Die Begriffe «Personendaten», «besonders schützenswerte Personendaten», «Bearbeitung», «Verantwortlicher», «Auftragsbearbeiter» und «Verletzung der Datensicherheit» haben die Bedeutung von Art. 5 DSGVO.

1.2 «Unterauftragsbearbeiter» ist ein Dritter, den Gallesis zur Bearbeitung von Personendaten des Verantwortlichen beizieht.

2. Gegenstand, Dauer, Art und Zweck

2.1 Gegenstand, Art, Zweck und Dauer der Bearbeitung sowie die Kategorien der Personendaten und der betroffenen Personen ergeben sich aus **Anlage A**.

2.2 Die Bearbeitung dauert so lange wie der Hauptvertrag. Sie endet mit dessen Beendigung; Ziff. 9 bleibt vorbehalten.

2.3 Gallesis bearbeitet die Personendaten ausschliesslich zur Erbringung der vertraglich geschuldeten Leistungen. Eine Nutzung für eigene Zwecke findet vorbehältlich Ziff. 2.4 nicht statt. Zur Verbesserung der Software darf Gallesis ausschliesslich anonymisierte Daten verwenden, die keinen Rückschluss auf den Verantwortlichen oder auf betroffene Personen zulassen.

2.4 Nicht Gegenstand dieses Vertrags sind Daten, die Gallesis als Verantwortliche bearbeitet: Vertrags-, Konto- und Abrechnungsdaten des Verantwortlichen und seiner Inhaberschaft, Zählwerte für die Preisberechnung sowie technische Zugriffsprotokolle (IP-Adresse, Zeitpunkt, aufgerufene Adresse) zur Sicherheit und Missbrauchsabwehr der Plattform. Dafür gilt die Datenschutzerklärung von Gallesis.

3. Weisungsgebundenheit

3.1 Gallesis bearbeitet die Personendaten nur auf dokumentierte Weisung des Verantwortlichen. Der Hauptvertrag und dieser Vertrag samt Anlagen gelten als vollständige Erstweisung; die Bedienung der Software durch den Verantwortlichen gilt als laufende Weisung.

3.2 Weisungen sind schriftlich zu erteilen (E-Mail genügt) an datenschutz@gallesis.com. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Weisungsberechtigt sind die Inhaberschaft des Verantwortlichen und die Personen, die im Kundenkonto die Rolle Inhaber oder Administration haben. Gallesis darf Weisungen anderer Personen zurückweisen.

3.3 Hält Gallesis eine Weisung für rechtswidrig, teilt sie dies dem Verantwortlichen unverzüglich mit und darf deren Ausführung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

3.4 Gallesis bearbeitet die Personendaten so, wie der Verantwortliche selbst es tun dürfte (Art. 9 Abs. 1 lit. a DSGVO). Der Verantwortliche bestätigt, dass keine gesetzliche oder vertragliche Geheimhaltungspflicht der Übertragung entgegensteht (Art. 9 Abs. 1 lit. b DSGVO); Ziff. 12 bleibt vorbehalten.

4. Vertraulichkeit

4.1 Gallesis verpflichtet alle Personen, die Zugang zu den Personendaten haben, schriftlich zur Vertraulichkeit; die Pflicht besteht über das Ende ihrer Tätigkeit hinaus.

4.2 Zugang erhält nur, wer ihn zur Aufgabenerfüllung braucht. Ein Zugriff auf Produktivdaten zu Supportzwecken erfolgt nur anlassbezogen, wird protokolliert und ist dem Verantwortlichen auf Anfrage offenzulegen.

5. Datensicherheit

5.1 Gallesis trifft die angemessenen technischen und organisatorischen Massnahmen nach Art. 8 DSGVO und Art. 1-6 DSV. Die bei Vertragsschluss geltenden Mindestvorkehrungen sind in **Anlage B** beschrieben.

5.2 Gallesis darf die Massnahmen weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird.

5.3 Der Verantwortliche hat sich vor Vertragsschluss vergewissert, dass Gallesis die Datensicherheit gewährleisten kann (Art. 9 Abs. 2 DSGVO); Anlage B dient diesem Nachweis.

6. Unterstützung des Verantwortlichen

6.1 **Rechte betroffener Personen.** Wendet sich eine betroffene Person direkt an Gallesis, leitet Gallesis die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst. Gallesis unterstützt den Verantwortlichen mit geeigneten technischen Mitteln bei der Erfüllung von Auskunfts-, Berichtigungs-, Löschungs- und Datenherausgabebegehren (Art. 25-28 und 32 DSGVO). Die Software stellt dafür je Kundin oder Kunde einen Export und eine Anonymisierung bereit, die Inhaberschaft und Administration nach einer Anmeldung mit Passwort auslösen können; die Anonymisierung lässt Buchungen und Belege bestehen und macht die Personenangaben unkenntlich.

6.2 **Verletzung der Datensicherheit.** Gallesis meldet dem Verantwortlichen jede Verletzung der Datensicherheit, die dessen Personendaten betrifft, **unverzüglich** nach Kenntnis, mit Angabe von Art und Zeitpunkt der Verletzung,

betroffenen Datenkategorien, möglichen Folgen und getroffenen Massnahmen. Die Meldung an den EDÖB und an betroffene Personen (Art. 24 DSG) obliegt dem Verantwortlichen; Galleis unterstützt ihn dabei.

6.3 Galleis unterstützt den Verantwortlichen auf dessen Verlangen bei einer Datenschutz-Folgenabschätzung (Art. 22 DSG) und bei einer allfälligen Konsultation des EDÖB, soweit die dafür nötigen Informationen bei Galleis liegen.

6.4 Galleis informiert den Verantwortlichen unverzüglich über behördliche Anordnungen, die die Herausgabe seiner Personendaten verlangen, sofern dies rechtlich zulässig ist, und widersetzt sich solchen Anordnungen im Rahmen des Zulässigen.

6.5 Der Verantwortliche meldet Galleis unverzüglich Vorfälle in seinem Bereich, welche die Plattform betreffen können, namentlich verlorene oder gestohlene Geräte und offengelegte Passwörter, PINs oder Gerätecodes.

7. Kontrollrechte

7.1 Der Verantwortliche kann sich von der Einhaltung dieses Vertrags überzeugen. Galleis erteilt dazu auf Anfrage Auskunft und stellt die verfügbaren Nachweise (Anlage B, Protokollauszüge, Berichte Dritter) zur Verfügung.

7.2 Galleis kann eine Kontrolle zunächst mit Unterlagen erfüllen (Anlage B, Bedingungen und Berichte der Unterauftragsbearbeiter, Protokollauszüge). Eine Kontrolle vor Ort ist nach vorgängiger Ankündigung von mindestens **30 Tagen** während der üblichen Geschäftszeiten und höchstens **einmal pro Kalenderjahr** möglich, ausser bei konkretem Verdacht auf eine Verletzung. Rechenzentren Dritter werden anhand der Unterlagen ihrer Betreiber geprüft. Die kontrollierende Person untersteht der Geheimhaltung und darf kein Wettbewerber von Galleis sein.

7.3 Der Verantwortliche trägt seine Kosten der Kontrolle. Den Aufwand von Galleis, der über die Bereitstellung vorhandener Unterlagen hinausgeht, trägt der Verantwortliche nach Aufwand; bei einer festgestellten wesentlichen Vertragsverletzung trägt ihn Galleis.

8. Bearbeitungsort und Bekanntgabe ins Ausland

8.1 Die Personendaten werden an den in **Anlage C** genannten Orten bearbeitet.

8.2 Die produktive Bearbeitung und Speicherung erfolgt heute in **Deutschland**. Deutschland gehört zu den Staaten mit angemessenem Datenschutz nach Anhang 1 der Datenschutzverordnung (DSV); eine Bekanntgabe dorthin bedarf keiner zusätzlichen Garantien.

8.3 Eine Bearbeitung in einem Staat ohne angemessenen Datenschutz findet nur statt, wenn geeignete Garantien nach Art. 16 Abs. 2 DSG bestehen, insbesondere die Standardvertragsklauseln der EU-Kommission in der vom EDÖB anerkannten Fassung mit den erforderlichen Anpassungen für die Schweiz. Die jeweils verwendeten Garantien sind in **Anlage D** dokumentiert.

8.4 Galleis informiert den Verantwortlichen vorgängig über eine Verlegung des Bearbeitungsorts.

9. Rückgabe und Löschung

9.1 Nach Beendigung des Hauptvertrags kann der Verantwortliche während **30 Tagen** die Exporte nach Ziff. 10.2 AGB abrufen. Einen Gesamtexport aller Personendaten schuldet Galleis nicht.

9.2 Danach löscht Galleis die Personendaten in den Produktivsystemen; die Löschung erfolgt heute von Hand. In den Sicherungskopien (Anlage B) bleiben sie enthalten, bis die jeweilige Sicherung abläuft: auf dem Server nach höchstens vier Wochen, in der verschlüsselten Kopie ausserhalb des Servers nach 30 bzw. 90 Tagen; monatliche Kopien werden derzeit ohne feste Löschfrist aufbewahrt. Bis dahin gelten die Pflichten dieses Vertrags weiter.

9.3 Von der Löschung ausgenommen sind Daten, deren Aufbewahrung Gallesis gesetzlich vorgeschrieben ist. Gallesis nennt dem Verantwortlichen diese Daten und den Grund.

9.4 Gallesis bestätigt die Löschung auf Verlangen schriftlich.

9.5 Übergibt der Verantwortliche seinen Betrieb einem Nachfolger, gibt Gallesis diesem Personendaten nur auf schriftliche Weisung des Verantwortlichen heraus (Ziff. 15.2 AGB).

10. Unterauftragsbearbeiter

10.1 Der Verantwortliche genehmigt hiermit den Beizug der in **Anlage E** aufgeführten Unterauftragsbearbeiter (allgemeine vorgängige Genehmigung nach Art. 9 Abs. 3 DSG).

10.2 Gallesis teilt jede beabsichtigte Änderung — Beizug eines neuen oder Ersetzung eines bestehenden Unterauftragsbearbeiters — dem Verantwortlichen mindestens **30 Tage** im Voraus schriftlich mit. Der Verantwortliche kann innert dieser Frist aus datenschutzrechtlichen Gründen begründet widersprechen. Hält Gallesis an der Änderung fest, kann der Verantwortliche den Hauptvertrag auf den Zeitpunkt der Änderung ausserordentlich und entschädigungslos kündigen.

10.3 Gallesis zieht nur Unterauftragsbearbeiter bei, die vertraglich zu Datenschutz und Datensicherheit verpflichtet sind. Schliesst ein Anbieter nur seine Standardbedingungen ab, gelten dessen Bedingungen zur Auftragsbearbeitung; Gallesis legt sie dem Verantwortlichen auf Verlangen vor.

10.4 Gallesis haftet für das Verhalten ihrer Unterauftragsbearbeiter wie für eigenes Verhalten.

11. Verzeichnis, Ansprechstelle

11.1 Gallesis führt ein Verzeichnis ihrer Bearbeitungstätigkeiten als Auftragsbearbeiterin nach Art. 12 Abs. 3 DSG und stellt dem Verantwortlichen auf Anfrage den ihn betreffenden Auszug zu.

11.2 Ansprechstelle für Datenschutzfragen bei Gallesis: datenschutz@gallesis.com.

12. Berufsgeheimnis (nur für Kunden mit Berufsgeheimnispflicht)

Bis ein Branchenanhang vereinbart ist, gilt Ziff. 1.7 AGB: Kunden mit Berufsgeheimnispflicht nutzen Gallesis nicht für Daten, die diesem Geheimnis unterliegen.

12.1 Untersteht der Verantwortliche einem Berufsgeheimnis (namentlich Art. 321 StGB für Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Apothekerinnen und Apotheker sowie deren Hilfspersonen), so wird Gallesis als **Hilfsperson** des Verantwortlichen beigezogen.

12.2 Gallesis und alle ihre Mitarbeitenden und Unterauftragsbearbeiter, die Zugang zu solchen Daten haben, sind zur Wahrung dieses Berufsgeheimnisses in gleichem Umfang verpflichtet wie der Verantwortliche und werden vor dem Zugang ausdrücklich darauf verpflichtet.

12.3 Gallesis gibt solche Daten nicht heraus, ohne den Verantwortlichen vorgängig zu informieren, damit dieser über eine Entbindung vom Berufsgeheimnis entscheiden kann.

12.4 Der Verantwortliche prüft in eigener Verantwortung, ob der Beizug von Gallesis nach den für ihn geltenden berufs- und kantonalrechtlichen Vorschriften zulässig ist.

13. Ausserordentliche Kündigung

Der Verantwortliche kann den Hauptvertrag und diesen Vertrag fristlos kündigen, wenn Gallesis schwer gegen Datenschutzvorschriften oder gegen diesen Vertrag verstösst, eine Weisung nicht ausführen kann oder will oder die Kontrollrechte nach Ziff. 7 vertragswidrig verweigert.

14. Schlussbestimmungen

14.1 Die Anlagen A-E sind integrierender Bestandteil dieses Vertrags.

14.2 Bei Widersprüchen zum Hauptvertrag geht dieser Vertrag in Fragen der Bearbeitung von Personendaten vor (Ziff. 1.6 AGB).

14.3 Die Bestimmungen dieses Vertrags gelten über die Beendigung des Hauptvertrags hinaus, solange Gallesis Personendaten des Verantwortlichen besitzt.

14.4 Änderungen bedürfen der Schriftform; E-Mail genügt.

14.5 Es gilt schweizerisches Recht unter Ausschluss der Kollisionsnormen des IPRG. Ausschliesslicher Gerichtsstand ist Luzern.

14.6 Für die Haftung aus diesem Vertrag gilt Ziff. 14 AGB; Ziff. 14.6 und 8.5 AGB gelten entsprechend.

Anlage A — Auftragsspezifizierung

Gegenstand und Zweck: Betrieb der Software Gallesis für den Verantwortlichen: Verkauf und Kassenführung, Bestellannahme über Theke, Selbstbedienungsterminal und Online-/QR-Seite, Küchensteuerung, Lieferung, Terminbuchung, Kunden- und Treueverwaltung, Lager und Einkauf, Personalplanung und Zeiterfassung, Auswertungen, Belegdruck sowie Buchhaltungs- und Steuerauszüge.

Art der Bearbeitung: Erheben, Speichern, Ordnen, Anzeigen, Verändern, Bekanntgeben an vom Verantwortlichen bestimmte Empfänger, Exportieren, Sichern, Anonymisieren, Löschen.

Dauer: Dauer des Hauptvertrags zuzüglich der Fristen nach Ziff. 9. Innerhalb dieser Dauer bestimmt der Verantwortliche, wie lange er Personendaten aufbewahrt; Kontaktangaben von Gästen bleiben gespeichert, bis der Verantwortliche sie löscht oder anonymisiert.

Kategorien betroffener Personen | Kategorie | Erfasst durch | I—I—I | Mitarbeitende des Verantwortlichen (inkl. Kuriere, Externe wie Treuhand und Lieferanten) | Benutzerkonten, Rollen, Dienstplan, Zeiterfassung | I | Kundinnen und Kunden, Gäste, bei Praxen: Patientinnen und Patienten | Kundenkartei, Bestellungen, Termine, Lieferungen | I | Besucherinnen und Besucher der öffentlichen Bestell- und Buchungsseiten | Onlinebestellung, Terminbuchung, Statusabfrage |

Kategorien von Personendaten | Kategorie | Beispiele | I—I—I | Kontakt- und Identifikationsdaten | Name, Telefonnummer, E-Mail-Adresse, Tischnummer, Zustelladresse | I | Transaktionsdaten | Bestellpositionen, Beträge, Zahlungsart, Steuerbetrag, Belegnummer, Trinkgeld | I | Notizen | Bestell- und Positionsnotizen, Kundennotiz, Terminnotiz (vom Personal erfasst) | I | Termin- und Leistungsdaten | Datum, Zeit, gebuchte Leistung, ausführende Person, Verlaufsstatus | I | Treuedaten | Punktestand, Buchungen, Einwilligung zur Teilnahme | I | Personaldaten | Name, E-Mail, Rolle, Schichten, Stempelzeiten, Stundenansatz und berechneter Lohn | I | Technische Daten | Anmeldeprotokolle, Gerätekennungen, IP-Adressen in Sicherheitsprotokollen, Prüfspur (Audit) | I | Nachrichtendaten | Versandte digitale Belege und Mitteilungen per E-Mail samt Empfängeradresse; SMS-Terminnachrichten (derzeit gesperrt) samt Mobilnummer |

Besonders schützenswerte Personendaten (Art. 5 lit. c DSGVO)

Grundsätzlich nicht vorgesehen. In folgenden Fällen können dennoch solche Daten anfallen und sind vom Verantwortlichen zu beachten: - **Gesundheitsbranche:** Die gebuchte Leistung (z. B. eine Therapieart) und Terminnotizen lassen Rückschlüsse auf die Gesundheit zu. - **Freitextfelder:** Notizfelder erlauben die Eingabe beliebiger Angaben. Der Verantwortliche weist sein Personal an, dort keine besonders schützenswerten Daten zu erfassen, soweit dies nicht erforderlich ist. - **Erährungs- und Glaubensbezug:** Bestellungen können mittelbar auf religiöse Überzeugungen hindeuten.

Nicht bearbeitet: Kartennummern und andere vollständige Zahlungsmitteldaten von Endkundinnen und Endkunden. Kartenzahlungen laufen über das eigene Zahlterminal bzw. den eigenen Zahlungsanbieter des Verantwortlichen. Schaltet der Verantwortliche eine Anbindung daran ein (z. B. Worldline, SumUp, Sitto bzw. Adyen), übermittelt Gallesis dem Anbieter in seinem Auftrag Betrag, Währung, Bestellnummer und Zahlungsreferenz und erhält den Zahlungsstatus zurück; Namen und Kontaktangaben werden nicht übermittelt, Kartendaten erhebt der Anbieter selbst. Der Anbieter ist Vertragspartner des Verantwortlichen und nicht Unterauftragsbearbeiter von Gallesis (Ziff. 2.6 AGB).

Anlage B — Technische und organisatorische Massnahmen (Mindestvorkehrungen)

Stand 11.10.2026. Raster nach Art. 3 DSV.

Vertraulichkeit - *Zugangskontrolle*: Server in einem Rechenzentrum mit Zutrittskontrolle des Betreibers; Administrationszugang ausschliesslich über SSH mit Schlüssel, Passwortanmeldung deaktiviert, Firewall auf die Ports 22/80/443 beschränkt. Automatische Sperre von Adressen nach wiederholten Fehlanmeldungen, gehärtete SSH-Konfiguration und automatische Sicherheitsaktualisierungen des Betriebssystems. - *Zugriffskontrolle*: Rollenbasierte Berechtigungen je Benutzerkonto; jede Berechtigung wird serverseitig geprüft; externe Rollen (Treuhand, Lieferant) sind auf eine ausdrückliche Liste erlaubter Aufrufe beschränkt. - *Benutzerkontrolle*: Persönliche Konten mit Passwort; neue Passwörter mit mindestens 12 Zeichen und nicht auf einer Liste häufiger Passwörter. Zwei-Faktor-Anmeldung (TOTP mit einmalig verwendbaren Wiederherstellungscodes) für die Konten von Gallesis Pflicht, für Inhaber-, Administrations- und Leitungskonten der Betriebe wählbar; die Geheimnisse dafür werden verschlüsselt gespeichert. Kassen-PIN für den Schichtbetrieb; gestaffelte Sperre nach wiederholten Fehlversuchen; Abmeldung aller Sitzungen bei Passwortwechsel oder Deaktivierung. - *Mandantentrennung*: Jeder Datensatz ist einem Mandanten zugeordnet; jede Abfrage ist auf den Mandanten des Tokens eingeschränkt.

Integrität und Verfügbarkeit - *Transportkontrolle*: Ausschliesslich TLS-verschlüsselte Verbindungen; automatische Umleitung von HTTP auf HTTPS; Sicherheits-Header inkl. Content Security Policy. - *Speicher- und Datenträgerkontrolle*: Passwörter und PINs nur als Hash (scrypt); die Geheimnisse der Zwei-Faktor-Anmeldung verschlüsselt. Die Sicherungen auf dem Produktivserver liegen **ohne zusätzliche Verschlüsselung** in einem nur dem Systemverwalter zugänglichen Verzeichnis; ihr Schutz beruht auf der Zugangskontrolle des Servers. Sicherungen, die den Server verlassen, werden vorher mit einem öffentlichen Schlüssel verschlüsselt (der private Schlüssel liegt nicht auf dem Server); ein unverschlüsselter Versand ist technisch ausgeschlossen. - *Wiederherstellung*: Stündliche Datenbanksicherung. Auf dem Server: stündliche Sicherungen 24 Stunden, tägliche 7 Tage, wöchentliche 4 Wochen. Ausserhalb des Servers: seit 20.09.2026 jede Stunde eine verschlüsselte Kopie bei Infomaniak (Swiss Backup) in der Schweiz, mit Prüfsumme über die verschlüsselte Datei; stündliche Kopien 30 Tage, wöchentliche 90 Tage, monatliche Kopien derzeit ohne feste Löschrfrist. Monatliche Wiederherstellungsprüfung der jüngsten Sicherung in eine Prüfdatenbank; vor jeder Softwareauslieferung eine zusätzliche Sicherung. - *Datenintegrität*: Geldrelevante Vorgänge laufen in Datenbanktransaktionen mit Wiederholungsschutz; Bestände und Punkte sind fortschreibende Journale ohne Überschreiben.

Nachvollziehbarkeit - *Eingabe- und Bekanntgabekontrolle*: Jede Änderung schreibt einen Prüfspureintrag (wer, wann, was) und ein Domänenereignis. Kontaktangaben von Gästen und Kundinnen und Kunden stehen nicht in Prüfspur, Ereignissen und Protokollen. Anfrageprotokolle und Prüfeinträge können IP-Adressen enthalten; beim Anlegen und Ändern eines Benutzerkontos enthält der Prüfeintrag Name und E-Mail-Adresse der Mitarbeiterin oder des Mitarbeiters. - *Erkennung*: Betriebskennzahlen und Bereitschaftsprüfung; Ratenbegrenzung auf Anmeldungen und allgemein pro IP-Adresse; Alarm-E-Mail bei Sicherheitsereignissen; Abhängigkeits-, Container- und statische Codeprüfung sowie Suche nach Geheimnissen in der Auslieferungskette; automatische Prüfung jeder Schnittstelle auf Anmeldung und Mandantentrennung; Container ohne Rechteauserweiterung und mit schreibgeschütztem Dateisystem; Abweisung von Kartennummern in Freitextfeldern.

Organisation - Schriftliche Vertraulichkeitsverpflichtung aller Zugangsberechtigten. - Dokumentierte Abläufe für Störungen, Wiederherstellung, Schlüsselwechsel und Datenschutzvorfälle. - Verfahren zur regelmässigen Überprüfung: periodische Sicherheits- und Berechtigungsdurchsichten vor grösseren Auslieferungen.

Bewusst nicht zugesichert: hochverfügbarer Betrieb, georedundante Speicherung, externe Zertifizierung (ISO 27001, SOC 2, PCI DSS) von Gallesis selbst.

Anlage C — Genehmigte Bearbeitungsorte

Ort	Land	Zweck	Angemessener Schutz
Rechenzentrum Düsseldorf	Deutschland	Produktivbetrieb, Datenbank, Dateiablage	ja (Anhang 1 DSV)
Infomaniak Swiss Backup	Schweiz	Ablage verschlüsselter Sicherungskopien ausserhalb des Produktivstandorts (seit 20.09.2026)	ja (Inland)
Arbeitsplatz der Auftragsbearbeiterin	Schweiz	Administration und Support	ja (Inland)
Rechenzentren von Infomaniak (E-Mail) und VADIAN.NET (SMS)	Schweiz	Versand von E-Mails und SMS	ja (Inland)

Anlage D — Geeignete Garantien für die Bekanntgabe ins Ausland

1. **Deutschland / EU-EWR:** keine zusätzlichen Garantien erforderlich (Anhang 1 DSV).
2. **USA:** nur zulässig, wenn der Empfänger unter dem **Swiss-U.S. Data Privacy Framework** zertifiziert ist (vom Bundesrat mit Wirkung ab 15. September 2024 als angemessen anerkannt), **oder** gestützt auf die Standardvertragsklauseln der EU-Kommission in der vom EDÖB anerkannten Fassung mit Schweizer Anpassungen. Die massgebliche Grundlage ist je Unterauftragsbearbeiter in Anlage E vermerkt.
3. **Übrige Staaten:** derzeit keine.
4. Gallesis dokumentiert die jeweils verwendeten Garantien und legt sie dem Verantwortlichen auf Verlangen vor.

Anlage E — Zugelassene Unterauftragsbearbeiter

Stand 11.10.2026. Änderungen nach Ziff. 10.2.

#	Unternehmen	Sitz / Bearbei- tungsort	Tätigkeit	Betroffene Daten	Grundla- ge
1	WIIT AG, Joachim-Erwin-Platz 3, 40212 Düsseldorf (Marke webtropia.com)	Düsseldorf, Deutschland	Betrieb des Servers und des Rechenzentrums (Infrastruktur)	alle in Anlage A genannten Daten	Anhang 1 DSV (DE)
2	Infomaniak Network SA	Genf, Schweiz	Ablage der verschlüsselten Sicherungskopien ausserhalb des Produktivstandorts (seit 20.09.2026)	verschlüsselte Gesamtsicherung; kein Klartextzugriff	Inland
3	Infomaniak Network SA	Genf, Schweiz	Versand von System-E-Mails (namentlich digitale Belege, Passwort- und Zugangsmitteilungen)	Empfängername, E-Mail-Adresse, Inhalt der Nachricht	Inland
4	VADIAN.NET AG (Dienst «ASPSMS»)	St. Gallen, Schweiz	Versand von SMS; Terminnachrichten per SMS sind derzeit gesperrt	Mobilnummer, Inhalt der Nachricht	Inland

Nicht Unterauftragsbearbeiter im Sinne dieses Vertrags: Der Zahlungsdienstleister, über den Gallesis das Abonnement des Verantwortlichen einzieht (**Stripe Payments Europe, Ltd.**, Irland, mit Konzerngesellschaften). Dieser bearbeitet ausschliesslich die Zahlungs- und Rechnungsdaten des Verantwortlichen als Vertragspartei von Gallesis, nicht Personendaten, für die der Verantwortliche verantwortlich ist. Er wird hier nur der Transparenz halber genannt.

Heute nicht angebunden: Lieferplattformen (Uber Eats, Just Eat). Zahlterminal- und Zahlungsanbieter, an die der Verantwortliche eine Anbindung einschaltet, sind seine eigenen Vertragspartner und keine Unterauftragsbearbeiter von Gallesis (Anlage A, «Nicht bearbeitet»). Kommt ein Unterauftragsbearbeiter hinzu, wird Anlage E nach Ziff. 10.2 ergänzt und dem Verantwortlichen mindestens 30 Tage im Voraus mitgeteilt.

Dieser Vertrag kommt durch die elektronische Annahme des Verantwortlichen im Bestellprozess oder im Kundenkonto zustande; Gallesis speichert die angenommene Fassung, den Zeitpunkt und die annehmende Person. Eine Unterschrift ist nicht erforderlich. Bei schriftlichem Abschluss: [Ort], [Datum] · Verantwortlicher: _____ · Gallesis: _____