

Vertrag zur Auftragsverarbeitung (AVV)

Für die Verarbeitung personenbezogener Daten im Auftrag von lokalen Betrieben, Gastronomie, Städten, Citymanagements, Einkaufscentern und sonstigen gewerblichen Nahlo-Kunden.

Stand: 27.09.2026

Dieser AVV gilt nur für Verarbeitungsvorgänge, bei denen Nahlo personenbezogene Daten im Auftrag des Kunden verarbeitet. Verarbeitungsvorgänge, für die Nahlo selbst Verantwortlicher ist, werden nicht durch diesen AVV geregelt.

Präambel und Vertragsschluss

(1) Dieser Vertrag zur Auftragsverarbeitung („AVV“) wird zwischen der CoaSoft - Consulting & Software UG (haftungsbeschränkt), Am Wäldchen 24, 66424 Homburg, Deutschland („Auftragsverarbeiter“, „Nahlo“) und dem jeweiligen gewerblichen Kunden („Verantwortlicher“ oder „Kunde“) geschlossen.

(2) Der AVV ergänzt den zwischen den Parteien bestehenden Hauptvertrag über die Nutzung von Nahlo, insbesondere die AGB, ein individuelles Angebot, einen Projektvertrag oder einen sonstigen Leistungsvertrag.

(3) Der AVV kann elektronisch abgeschlossen werden, insbesondere durch ausdrückliche Zustimmung im Dashboard, im digitalen Onboarding, im Bestellprozess oder durch elektronische Annahme eines Angebots. Der Vertrag wird in elektronischer Form bereitgestellt.

(4) Soweit der Kunde seinerseits als Auftragsverarbeiter für einen Dritten handelt, gilt er im Rahmen dieses AVV als Auftragsverarbeiter und Nahlo als weiterer Auftragsverarbeiter (Sub-Auftragsverarbeiter), soweit dies für den jeweiligen Verarbeitungsvorgang zutrifft. Der Kunde sichert zu, über die hierfür erforderliche Beauftragung beziehungsweise Genehmigung seines Verantwortlichen zu verfügen.

§ 1 Gegenstand, Dauer und Rangfolge

(1) Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch Nahlo im Auftrag des Kunden im Zusammenhang mit den im Hauptvertrag vereinbarten Nahlo-Leistungen, einschließlich des Website-Baukastens zur Erstellung und zum Hosting von Händler-Landingpages unter von Nahlo vergebenen Shop-URLs auf der Domain app.nahlo.de (Pfad /s/:slug), Widgets sowie der Gastro-Bestellfunktion (Live-Speisekarte, In-Chat-Bestellung, Bestellübersicht, Bon-Benachrichtigungen), des Kontakt- und Nachrichtenübermittlungsmoduls (Contact Messages), der Terminanfragen-Funktion sowie der Kalender- und Mitarbeiterverwaltung, soweit dabei personenbezogene Daten im Auftrag des Kunden verarbeitet werden.

(2) Die Verarbeitung dauert grundsätzlich so lange wie der Hauptvertrag beziehungsweise so lange, wie Nahlo im Rahmen des Hauptvertrages personenbezogene Daten im Auftrag des Kunden verarbeitet. Pflichten, die ihrer Natur nach über das Vertragsende hinaus fortgelten, bleiben unberührt.

(3) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV für Fragen der Auftragsverarbeitung vor. Ein gesondert vereinbarter datenschutzrechtlicher Individualvertrag geht diesem AVV vor.

§ 2 Abgrenzung der Datenschutzrollen

(1) Dieser AVV gilt ausschließlich für Verarbeitungsvorgänge, bei denen der Kunde Zwecke und wesentliche Mittel der Verarbeitung festlegt und Nahlo personenbezogene Daten auf dokumentierte Weisung des Kunden verarbeitet.

(2) Je nach konkret genutzter Funktion können unterschiedliche datenschutzrechtliche Rollen bestehen. Insbesondere kann Nahlo bestimmte personenbezogene Daten als eigenständig Verantwortlicher verarbeiten, soweit Nahlo die Zwecke und wesentlichen Mittel dieser Verarbeitung selbst festlegt.

(3) Nicht Gegenstand dieses AVV sind insbesondere Verarbeitungsvorgänge, die Nahlo ausschließlich für eigene Vertragsverwaltung, gesetzliche Aufbewahrungspflichten, Buchhaltung, Forderungsmanagement, eigene IT-Sicherheit oder Missbrauchsprävention als Verantwortlicher durchführt, soweit Nahlo hierbei nicht auf Weisung des Kunden tätig wird.

(4) Die Nutzung eines externen Zahlungsdienstleisters für die Abrechnung ist nicht allein deshalb Teil dieses AVV. Die datenschutzrechtlichen Rollen richten sich nach der jeweils konkreten Zahlungsdienstleistung und den hierfür geltenden Vertragsbedingungen. Bei Zahlungen über Stripe Connect im Modul Gastro-Bestellung fungiert der Kunde als Verkäufer und Stripe als dessen eigenständiger Zahlungsdienstleister; Nahlo verarbeitet in diesem Kontext lediglich die zugehörigen Bestellstammdaten im Auftrag.

§ 3 Einzelheiten der Verarbeitung

Art, Zweck, Gegenstand, Kategorien personenbezogener Daten und Kategorien betroffener Personen ergeben sich aus Anlage 1 – Beschreibung der Verarbeitung. Anlage 1 ist Bestandteil dieses AVV.

§ 4 Weisungsgebundenheit

(1) Nahlo verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Kunden, einschließlich hinsichtlich Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern Nahlo nicht durch Unionsrecht oder das Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet ist.

(2) Ist Nahlo gesetzlich zu einer Verarbeitung verpflichtet, wird Nahlo den Kunden vor der Verarbeitung über die betreffende rechtliche Anforderung informieren, soweit das anwendbare Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

(3) Dokumentierte Weisungen ergeben sich insbesondere aus dem Hauptvertrag, diesem AVV und aus Handlungen berechtigter Nutzer im Dashboard, etwa Upload, Freigabe, Änderung, Löschung, Export, Bearbeitung von Website-Inhalten oder Konfiguration von Integrationen.

(4) Zusätzliche Weisungen können in Textform übermittelt werden. Entstehen dadurch Leistungen, die über den vereinbarten Leistungsumfang hinausgehen, können die Parteien vor der Umsetzung eine gesonderte Vergütung vereinbaren.

(5) Ist Nahlo der Auffassung, dass eine Weisung gegen Datenschutzrecht verstößt, informiert Nahlo den Kunden unverzüglich. Nahlo darf die Durchführung der betreffenden Weisung aussetzen, bis sie bestätigt, geändert oder ihre Rechtmäßigkeit geklärt wurde.

§ 5 Pflichten von Nahlo als Auftragsverarbeiter

Nahlo verpflichtet sich insbesondere,

- personenbezogene Daten nur im vereinbarten Umfang und auf dokumentierte Weisung zu verarbeiten;

- sicherzustellen, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO umzusetzen und aufrechtzuerhalten;
- die Voraussetzungen für die Hinzuziehung weiterer Auftragsverarbeiter gemäß § 8 einzuhalten;
- den Kunden unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Betroffenenrechten zu unterstützen;
- den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO zu unterstützen;
- nach Maßgabe von § 13 personenbezogene Daten nach Ende der Auftragsverarbeitung zu löschen oder zurückzugeben;
- dem Kunden die erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung zu stellen und Überprüfungen nach Maßgabe von § 10 zu ermöglichen.

§ 6 Pflichten des Kunden

- (1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für eine erforderliche Rechtsgrundlage, Informationspflichten, Löschkonzepte und die Wahrung der Rechte betroffener Personen verantwortlich, soweit diese Pflichten nach Datenschutzrecht beim Verantwortlichen liegen.
- (2) Der Kunde darf Nahlo nur personenbezogene Daten zur Verarbeitung bereitstellen, deren Verarbeitung im Rahmen des Hauptvertrages rechtmäßig ist. Das gilt insbesondere auch für Impressumsangaben und sonstige auf gehosteten Händler-Websites veröffentlichte personenbezogene Inhalte.
- (3) Der Kunde informiert Nahlo unverzüglich, wenn er Fehler, Unregelmäßigkeiten oder datenschutzrechtlich relevante Besonderheiten in der Auftragsverarbeitung feststellt.
- (4) Soweit besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO oder Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Art. 10 DSGVO verarbeitet werden sollen, ist dies vorab ausdrücklich mit Nahlo abzustimmen, sofern eine solche Verarbeitung nicht bereits ausdrücklich im Hauptvertrag vorgesehen ist.

§ 7 Technische und organisatorische Maßnahmen

- (1) Nahlo trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die zum Zeitpunkt des Vertragsschlusses vorgesehenen Maßnahmen ergeben sich aus Anlage 2 – Technische und organisatorische Maßnahmen (TOM).
- (2) Die TOM dürfen im Rahmen des technischen Fortschritts und der Weiterentwicklung der Plattform angepasst werden, sofern das vereinbarte Schutzniveau dadurch insgesamt nicht herabgesetzt wird.
- (3) Sicherheitsmaßnahmen von eingesetzten Cloud- und Infrastrukturanbietern werden im Rahmen des Shared-Responsibility-Modells berücksichtigt.

§ 8 Weitere Auftragsverarbeiter (Unterauftragnehmer)

- (1) Der Kunde erteilt Nahlo die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter einzusetzen, soweit dies zur Erbringung der vereinbarten Leistungen erforderlich ist.
- (2) Die bei Abschluss dieses AVV vorgesehenen weiteren Auftragsverarbeiter sind in Anlage 3 – Unterauftragnehmer aufgeführt.
- (3) Nahlo informiert den Kunden über beabsichtigte Änderungen bei der Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter mit angemessenem Vorlauf, grundsätzlich mindestens 14 Tage vor Beginn der betreffenden Verarbeitung, soweit nicht aus Sicherheits-, Verfügbarkeits- oder sonstigen zwingenden Gründen eine kurzfristigere Änderung erforderlich ist.
- (4) Der Kunde kann einer Änderung aus einem nachvollziehbaren datenschutzrechtlichen Grund innerhalb der mitgeteilten Frist widersprechen. Die Parteien werden sich in diesem Fall um eine zumutbare Lösung bemühen. Ist eine solche nicht möglich und kann Nahlo die Leistung ohne den betreffenden Unterauftragnehmer nicht zumutbar erbringen, können die Parteien den betroffenen Leistungsteil beziehungsweise den Vertrag nach Maßgabe des Hauptvertrages beenden.
- (5) Nahlo verpflichtet weitere Auftragsverarbeiter vertraglich zu Datenschutzpflichten, die den für die jeweilige Verarbeitung relevanten Pflichten dieses AVV entsprechen. Nahlo bleibt gegenüber dem Kunden für die Erfüllung der Pflichten des weiteren Auftragsverarbeiters im Rahmen der gesetzlichen Vorgaben verantwortlich.
- (6) Ein externer Dienst wird nur dann als Unterauftragnehmer im Rahmen dieses AVV eingesetzt, wenn für die betreffende Verarbeitung eine datenschutzrechtlich geeignete vertragliche Grundlage besteht. Optionale Kommunikationskanäle oder Drittplattformen, für die eine erforderliche Auftragsverarbeitungsbeziehung oder ein erforderlicher Transfermechanismus nicht sichergestellt ist, sind nicht Teil der Auftragsverarbeitung nach diesem AVV.

§ 9 Drittlandübermittlungen

- (1) Soweit personenbezogene Daten im Rahmen der Auftragsverarbeitung in ein Land außerhalb des Europäischen Wirtschaftsraums übermittelt werden oder ein Zugriff aus einem solchen Land erfolgt, stellt Nahlo sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden.
- (2) Je nach Empfänger und Verarbeitung können hierfür insbesondere ein Angemessenheitsbeschluss der Europäischen Kommission, von der Europäischen Kommission genehmigte Standardvertragsklauseln oder ein anderer gesetzlich anerkannter Transfermechanismus eingesetzt werden.
- (3) Soweit erforderlich, werden ergänzende Maßnahmen und Informationen zur Drittlandübermittlung im Rahmen der jeweiligen Anbieter- und Transferdokumentation berücksichtigt.

§ 10 Nachweise, Informations- und Auditrechte

- (1) Nahlo stellt dem Kunden auf Anfrage die Informationen zur Verfügung, die vernünftigerweise erforderlich sind, um die Einhaltung der Pflichten aus diesem AVV und Art. 28 DSGVO nachzuweisen.
- (2) Der Nachweis kann insbesondere durch aktuelle Datenschutz- und Sicherheitsdokumentationen, TOM, Prüfberichte, Zertifizierungen oder geeignete Nachweise eingesetzter Infrastruktur- und Unterauftragnehmer erfolgen.

(3) Reichen diese Nachweise im konkreten Fall nicht aus, kann der Kunde nach angemessener Vorankündigung eine weitergehende Prüfung selbst oder durch einen unabhängigen, zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Prüfungen sind so auszugestalten, dass Betriebsabläufe, Sicherheitsinteressen, Geschäftsgeheimnisse und Rechte anderer Kunden angemessen geschützt werden.

(4) Vor-Ort-Prüfungen sollen grundsätzlich mindestens 14 Werktage vorher angekündigt und während üblicher Geschäftszeiten durchgeführt werden, soweit kein datenschutzrechtlicher Vorfall oder eine behördliche Anordnung eine kurzfristigere Prüfung erforderlich macht.

(5) Jede Partei trägt grundsätzlich ihre eigenen Kosten der Prüfung. Verursacht der Kunde außergewöhnlichen, nicht durch einen konkreten Verdacht oder Verstoß veranlassten Zusatzaufwand, kann eine angemessene Vergütung hierfür nur nach vorheriger Abstimmung verlangt werden. Gesetzliche Auditrechte dürfen dadurch nicht unangemessen erschwert werden.

§ 11 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Erlangt Nahlo Kenntnis von einer Verletzung des Schutzes personenbezogener Daten, die im Rahmen dieses AVV im Auftrag verarbeitet werden, informiert Nahlo den Kunden unverzüglich.

(2) Soweit verfügbar, enthält die Mitteilung die Informationen, die der Kunde vernünftigerweise benötigt, um seine Pflichten nach Art. 33 und 34 DSGVO zu beurteilen und zu erfüllen, insbesondere Art des Vorfalls, betroffene Datenkategorien, mögliche Folgen und bereits ergriffene oder vorgeschlagene Abhilfemaßnahmen.

(3) Können Informationen nicht gleichzeitig bereitgestellt werden, dürfen sie ohne unangemessene weitere Verzögerung schrittweise ergänzt werden.

§ 12 Betroffenenrechte, Datenschutz-Folgenabschätzung und Behörden

(1) Erhält Nahlo eine Anfrage einer betroffenen Person, die erkennbar eine Verarbeitung im Auftrag des Kunden betrifft, wird Nahlo die Anfrage grundsätzlich an den Kunden weiterleiten oder die betroffene Person an den Kunden verweisen, soweit Nahlo nicht zur eigenständigen Bearbeitung berechtigt oder verpflichtet ist.

(2) Nahlo unterstützt den Kunden im Rahmen der technischen Möglichkeiten bei Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch und sonstigen einschlägigen Betroffenenrechten.

(3) Nahlo unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei einer gegebenenfalls erforderlichen Datenschutz-Folgenabschätzung sowie bei einer Konsultation der Aufsichtsbehörde nach Art. 35 und 36 DSGVO.

§ 13 Rückgabe und Löschung nach Vertragsende

(1) Nach Beendigung der Auftragsverarbeitung löscht oder gibt Nahlo die im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Kunden zurück, soweit nicht eine gesetzliche Pflicht zur weiteren Speicherung besteht.

(2) Soweit die Plattform eine Exportfunktion vorsieht, kann der Kunde diese bis zur Beendigung des Zugriffs nutzen. Besondere Exportformate oder individuelle Migrationsleistungen sind nur geschuldet, wenn sie vereinbart wurden.

(3) Produktive Daten werden nach Vertragsende innerhalb des technisch vorgesehenen Löschmods gelöscht, grundsätzlich innerhalb von 30 Tagen, sofern keine abweichende Vereinbarung, gesetzliche Aufbewahrungspflicht oder fortbestehende Verarbeitungsgrundlage besteht.

(4) Daten in technischen Sicherungskopien können bis zum Ablauf des regulären Backup-Rotationszyklus fortbestehen. Sie werden währenddessen nicht für den regulären Produktivbetrieb wiederverwendet und mit Ablauf des Rotationszyklus überschrieben beziehungsweise gelöscht. Der derzeit vorgesehene maximale Rotationszeitraum beträgt 90 Tage, soweit die konkret eingesetzte Infrastruktur keinen kürzeren Zeitraum vorsieht.

(5) Nachweise und Abrechnungsbelege, die Nahlo aufgrund eigener gesetzlicher Pflichten (insbesondere steuer- und handelsrechtliche Aufbewahrungsfristen nach § 147 AO und § 257 HGB) als Verantwortlicher aufbewahren muss, fallen nicht unter eine Weisung zur sofortigen Löschung nach diesem AVV.

§ 14 Schlussbestimmungen

(1) Änderungen dieses AVV einschließlich seiner Anlagen können in elektronischer Form vereinbart werden.

(2) Änderungen technischer und organisatorischer Maßnahmen oder der Unterauftragnehmer-Liste richten sich nach den hierfür in diesem AVV vorgesehenen Verfahren und bedürfen nicht jedes Mal eines vollständigen Neuabschlusses des AVV.

(3) Es gilt das Recht der Bundesrepublik Deutschland, soweit dies datenschutzrechtlich zulässig ist. Zwingende datenschutzrechtliche Vorschriften bleiben unberührt.

(4) Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleiben die übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung treten die anwendbaren gesetzlichen Vorschriften.

Anlage 1

Beschreibung der Verarbeitung

Gegenstand

Bereitstellung und Betrieb der im Hauptvertrag vereinbarten Nahlo-Funktionen, soweit hierbei personenbezogene Daten im Auftrag des Kunden verarbeitet werden.

Dauer

Für die Dauer des Hauptvertrages sowie für technisch oder gesetzlich erforderliche Abwicklungs- und Löschräume.

Art und Zweck

Erheben beziehungsweise Entgegennehmen, Speichern, Ordnen, Strukturieren, Auslesen, Abgleichen, Verarbeiten, Bereitstellen, Übermitteln, Weiterleiten, Löschen und – soweit vereinbart – KI-gestützte Analyse zur Bereitstellung von Such-, Chat-, Dashboard-, Widget-, Portal- und Website-Baukasten-Funktionen einschließlich Hosting von Händler-Landingpages, Entgegennahme von Kontaktanfragen und Abwicklung von Gastro-Bestellungen.

Verarbeitungsvorgänge

Insbesondere Nutzer- und Teamverwaltung, Dokumentenverarbeitung, Pflege und Veröffentlichung von Wissensdaten, technische Bereitstellung von Such- und Chat-Funktionen, Hosting und Auslieferung von Händler-Landingpages unter Shop-URLs auf app.nahlo.de/s/:slug, Entgegennahme, Weiterleitung und Benachrichtigung von Gastro-Bestellungen (Küchen-Dashboard, Bon-E-Mails), Weiterleitung von Kontaktnachrichten (Contact Messages), Verwaltung von Terminanfragen einschließlich Kalender-, Slot- und Mitarbeiterblöcken, Versand transaktionaler Benachrichtigungs-E-Mails, Protokollierung, Fehleranalyse und vom Kunden

ausgelöste Exporte oder Löschungen.

Kategorien personenbezogener Daten

- Account- und Teamdaten: Name, geschäftliche E-Mail-Adresse, Benutzerkennung, Rolle, Berechtigungen und gegebenenfalls Organisationseinheit.
- Geschäftliche Kontakt- und Profildaten: Ansprechpartner, geschäftliche Telefonnummern, E-Mail-Adressen und sonstige personenbezogene Angaben, die der Kunde in Profilen, Verzeichnissen oder Inhalten bereitstellt.
- Inhalts- und Dokumentdaten: personenbezogene Daten, die in hochgeladenen Dokumenten, Freitexten, Importen, Speisekarten, Sortimentslisten, Website-Inhalten, Impressumsangaben oder sonstigen Datenquellen enthalten sind.
- Interaktions- und Kontaktdaten (Contact Messages): Such- oder Chat-Eingaben, Absender-E-Mail-Adresse, Name des Anfragenden und Nachrichtentext bei Kontaktformularen sowie damit verbundene Metadaten.
- Bestell- und Terminkundendaten: Name, E-Mail-Adresse, Telefonnummer, optional Lieferadresse und Lieferhinweise, Bestellpositionen, Zahlungsart, Zahlungsstatus sowie zugehörige Stripe-Transaktions-IDs (ohne Roh-Kreditkartendaten), gewünschte Zeitslots, Mitarbeiterpräferenz, Notizen sowie Bearbeitungsstatus von Terminanfragen und Bestellungen, soweit diese im Auftrag des Kunden über Nahlo verarbeitet werden.
- Technische Daten: IP-Adresse, Zeitstempel, Geräte-/Browserinformationen, Authentifizierungs- und Sicherheitsereignisse sowie Zugriffsprotokolle gehosteter Händler-Websites und Widgets, soweit diese Verarbeitung im konkreten Fall dem Kunden zuzurechnen und Gegenstand der Auftragsverarbeitung ist.

Kategorien betroffener Personen

- Mitarbeiter, Beauftragte und Teammitglieder des Kunden,
- teilnehmende Händler, Gastronomiebetriebe und sonstige lokale Betriebe sowie deren Ansprechpartner,
- städtische, kommunale oder Center-Ansprechpartner,
- Endkunden, Gäste und Seitenbesucher, welche über die Plattform Bestellungen aufgeben, Kontaktanfragen stellen oder Such- und Chat-Funktionen sowie gehostete Händler-Landingpages unter Shop-URLs auf app.nahlo.de/s/:slug nutzen,
- sonstige Personen, deren Daten der Kunde rechtmäßig in die Plattform einstellt.

Besondere Kategorien personenbezogener Daten

Die planmäßige Erhebung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO ist nicht Bestandteil der Standardleistung. Endkunden können jedoch freiwillig Allergie- oder Unverträglichkeitsangaben in Bestellnotizen oder Sonderwünschten mitteilen. Der Kunde verarbeitet solche Angaben nur zur Bearbeitung der jeweiligen Bestellung, beschränkt den Empfängerkreis auf das zuständige Personal und löscht sie mit der Bestellung, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Eine darüber hinausgehende Verarbeitung besonderer Kategorien bedarf einer gesonderten Prüfung und Vereinbarung.

Anlage 2

Technische und organisatorische Maßnahmen (TOM)

Die nachfolgenden Maßnahmen beschreiben das vorgesehene Schutzniveau. Konkrete technische Implementierungen dürfen weiterentwickelt oder durch mindestens gleichwertige Maßnahmen ersetzt werden.

1. Vertraulichkeit und Zugriffsschutz

- rollen- und berechtigungsbasierte Zugriffskontrollen,
- Mandantentrennung und logische Trennung von Kundendaten,
- Authentifizierungs- und Verifizierungsverfahren für administrative Zugriffe,
- Prinzip der erforderlichen Berechtigung („Need to know“),
- Verpflichtung berechtigter Personen auf Vertraulichkeit.

2. Verschlüsselung und Übertragung

- verschlüsselte Datenübertragung über HTTPS/TLS nach aktuellem Stand der Technik,
- Verschlüsselung ruhender Daten durch die eingesetzten Infrastruktur- und Cloud-Dienste, soweit für den jeweiligen Dienst vorgesehen,
- Schutz von Zugangsdaten, Tokens und Geheimnissen vor unbefugter Offenlegung.

3. Integrität und Systemsicherheit

- technische Validierung und Zugriffsbeschränkung auf APIs,
- Protokollierung sicherheitsrelevanter Ereignisse in angemessenem Umfang,
- Rate-Limiting oder vergleichbare Schutzmaßnahmen gegen missbräuchliche automatisierte Zugriffe, soweit technisch eingesetzt,
- regelmäßige Sicherheits- und Systemupdates der kontrollierten Komponenten.

4. Verfügbarkeit und Wiederherstellung

- Nutzung geeigneter Cloud-Infrastruktur mit Maßnahmen zur Verfügbarkeit und Belastbarkeit,
- Datensicherungs- beziehungsweise Wiederherstellungsmechanismen entsprechend der eingesetzten Dienste,
- Monitoring und Fehleranalyse zur Erkennung betrieblicher Störungen.

5. Datenschutzfreundliche Verarbeitung

- Beschränkung der Verarbeitung auf die für die Leistung erforderlichen Daten,
- Freigabemechanismen für öffentlich verwendete Kundeninhalte, soweit im Produkt vorgesehen,
- Lösch- und Exportmöglichkeiten im Rahmen der angebotenen Funktionen,
- Trennung von Entwurfs- und veröffentlichten Inhalten, soweit technisch vorgesehen.

6. Überprüfung und Verbesserung

- regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen im Rahmen der Produkt- und Sicherheitsentwicklung,
- Anpassung an wesentliche Änderungen der Risikolage, Infrastruktur oder gesetzlichen Anforderungen,
- Einbeziehung geeigneter Sicherheitsnachweise der eingesetzten Cloud- und Infrastrukturprovider.

Anlage 3

Unterauftragnehmer

Die folgende Liste bildet die auf Grundlage der derzeitigen technischen Architektur vorgesehenen Anbieter ab, soweit sie bei der konkreten Nutzung personenbezogene Daten im Auftrag von Nahlo für den Kunden verarbeiten. Der tatsächliche Einsatz kann vom gebuchten Leistungsumfang abhängen.

Nicht pauschal als Unterauftragnehmer dieser AVV-Liste eingeordnet:

Stripe: Zahlungsdienstleistungen können je nach Verarbeitung sowohl Auftragsverarbeiter- als auch eigenständige Verantwortlichenrollen beinhalten. Bei Stripe Connect für Endkunden-Zahlungen im Rahmen von Gastro-Bestellungen handelt Stripe als eigenständiger Zahlungsdienstleister; Nahlo verarbeitet die Bestellstammdaten (Name, Kontakt, Lieferadresse) im Auftrag des Kunden. Stripe wird daher nicht pauschal als Unterauftragsverarbeiter des Kunden unter diesem AVV eingeordnet.

Optionale externe Kommunikationskanäle (z. B. Telegram): Solche Dienste werden für eine Auftragsverarbeitung personenbezogener Kundendaten nur eingesetzt, wenn die erforderliche datenschutzrechtliche Rollenklärung, vertragliche Absicherung und gegebenenfalls Drittlandtransfergrundlage vorliegt. Andernfalls sind sie nicht Bestandteil der durch diesen AVV abgedeckten Auftragsverarbeitung.

Die Unterauftragnehmer-Liste muss bei Änderungen der Produktionsarchitektur aktualisiert werden. Maßgeblich ist, welcher Dienst im jeweiligen Produktivsystem tatsächlich personenbezogene Daten im Auftrag verarbeitet.