# Auftragsbearbeitungsvertrag (AVV)

Stand: 8. November 2026 · Version 2026-11-06

Vertragspartnerin und Rechnungsstellerin ist die Betreiberin (noowy, Patrice Gobat & Nicolas Affolter (einfache Gesellschaft)); Wichtli ist eine Marke von ihr.

Version 2026-11-06. Zwischen der Kundin (Verantwortliche) und noowy, Patrice Gobat & Nicolas Affolter (einfache Gesellschaft) (Auftragsbearbeiterin, «wir»). Der AVV ist Anhang 1 der AGB und wird im Checkout akzeptiert; Version und Zeitpunkt speichern wir mit der Bestellung.

## 1. Gegenstand und Dauer

Wir bearbeiten Personendaten im Auftrag der Kundin, um eine Wichtli-Runde durchzuführen. Der AVV gilt für die Dauer der Runde und bis zur Löschung der Daten nach Ziffer 11.

## 2. Art und Zweck

Einladung, freiwillige Anmeldung, Auslosung, anonymer Chat, Adventskalender, Enthüllung, Bericht und bestellte Extras (inkl. Lieferung). Keine Nutzung für Werbung oder eigene Zwecke; Statistiken nur aggregiert.

## 3. Datenarten

- Name, Arbeits-E-Mail, optional Team, Standort, E-Mail der vorgesetzten Person;
- Zusage, Auslosung, Fragebogen, Hinweise, Fun Fact;
- Inhalt und Metadaten von Nachrichten im anonymen Chat;
- Postkarten: Vor- und Nachname und Büroadresse der Empfängerin oder des Empfängers, Motiv mit Vorname, Kartentext;
- Wohnadresse (freiwillig oder bei bestellter Lieferung, verschlüsselt).

## 4. Betroffene Personen

Mitarbeitende und weitere von der Kundin eingeladene Personen sowie ihre Admins.

## 5. Weisungen

Wir bearbeiten die Daten nur auf dokumentierte Weisung der Kundin; die Einstellungen der Runde gelten als Weisung. Wir informieren die Kundin, wenn eine Weisung nach unserer Auffassung gegen Datenschutzrecht verstösst.

Stehende Weisung: «Prüfung ausschliesslich gemeldeter Nachrichten; Offenlegung der Identität des Absenders nur auf schriftliches Verlangen der in der Runde hinterlegten HR-Kontaktperson nach einer Meldung; Protokollierung.» Behörden geben wir Daten nur auf gültige Anordnung heraus.

## 6. Vertraulichkeit

Alle Personen, die bei uns Zugriff auf die Daten haben, sind zur Vertraulichkeit verpflichtet.

## 7. Technische und organisatorische Massnahmen (Anhang 2, TOM)

- Datensparsamkeit: nur die nötigen Felder; Voreinstellungen privat.
- Transportverschlüsselung (TLS) für alle Verbindungen; HSTS.
- Speicherung in Cloudflare D1 mit EU-Jurisdiktion.
- Wohnadressen: AES-256-GCM-Verschlüsselung pro Datensatz mit firmenspezifisch abgeleitetem Schlüssel; Schlüssel nur als Worker-Secret, nie im Code.
- Kein Endpunkt liest Adressen aus; entschlüsselt wird nur im Versandexport, jede Entschlüsselung wird protokolliert (wer, wann, ohne Adresse).
- HR und Admins sehen nie, wer wen gezogen hat, keine Fragebogen-Antworten und keine Nachrichten.
- Rollenbasierter Zugriff; Zwei-Faktor-Authentisierung für den Betreiber-Zugang; Anmeldung per Einmal-Link.
- Logs ohne Inhalte und ohne Adressen; Aufbewahrung 30 Tage.
- E-Mails enthalten nie Paare, Namen des Wichtelkinds oder Wichtels und standardmässig keinen Nachrichtentext. Absenderdomain mit SPF, DKIM und DMARC.
- Automatische Löschung nach Ziffer 11; Backups verfallen nach höchstens 30 Tagen.
- Vorfallprozess: eindämmen, bewerten, protokollieren; Protokoll der Verletzungen 2 Jahre.

## 8. Unterauftragsbearbeiter (Anhang 3)

Die Kundin genehmigt die folgenden Unterauftragsbearbeiter. Neue oder geänderte Unterauftragsbearbeiter kündigen wir 30 Tage im Voraus per E-Mail an; die Kundin kann aus wichtigem datenschutzrechtlichem Grund widersprechen und, wenn wir keine Lösung finden, den Vertrag für künftige Leistungen kündigen. Wir verpflichten Unterauftragsbearbeiter vertraglich auf gleichwertige Pflichten.

Unterauftragsbearbeiter

Anbieter · Zweck · Sitz · Speicherung / Verarbeitung · Transfermechanismus · Status

Cloudflare Inc. (Workers, D1, R2, CDN) · Hosting, Datenbank · USA (Muttergesellschaft) · Speicherung in der EU (D1 EU-Jurisdiktion); weltweites Edge-Netz · DPF (EU-US, Swiss-US) + Standardvertragsklauseln im Cloudflare-AVV · aktiv

Cloudflare Email Service · Transaktions-E-Mails, Chat-Weiterleitung · USA (Muttergesellschaft) · weltweites Edge-Netz, nur Durchleitung · DPF + Standardvertragsklauseln (Cloudflare-AVV) · aktiv

Stripe Payments Europe Ltd. / Stripe Inc. · Zahlung (geschäftliche Kontaktdaten + Kartendaten; Stripe ist für die Zahlungs-Compliance selbst Verantwortliche) · IE / USA · EU/US · Stripe ist unter dem EU-US DPF inkl. Swiss-US DPF zertifiziert; Data Transfers Addendum als Rückfallebene · noch nicht aktiv

Gelato (print, gift, home delivery) · Verarbeitung von Name und Adresse der Empfängerin oder des Empfängers · NO (EWR) · CH/EU/EWR, erst nach schriftlicher Bestätigung (AVV oder API-Einstellung) vor der Aktivierung; die Unterauftragsbearbeiter von Gelato werden vor der Aktivierung hier aufgeführt oder verlinkt · EWR, angemessen; unterzeichneter AVV vor der Aktivierung · noch nicht aktiv

Prodigi Group Ltd (print, backup) · Verarbeitung von Name und Adresse der Empfängerin oder des Empfängers · UK · UK, EU; CH/EU/EWR/UK erst nach schriftlicher Bestätigung vor der Aktivierung · Angemessenheit UK (CH und EU) · noch nicht aktiv

Die Post (Swiss Post) · Druck und Versand von Postkarten: Name und Büroadresse der Empfängerin oder des Empfängers, Vorname auf der Vorderseite, Kartentext · CH · CH, erst nach schriftlicher Bestätigung vor der Aktivierung · nicht nötig (Inland) · noch nicht aktiv

Anbieter für KI-/GIF-Erstellung (falls genutzt) · personalisierte GIFs · noch nicht gewählt · noch nicht gewählt · nur mit AVV; zum Start keine echten Fotos von Personen, nur textbasierte Personalisierung · noch nicht aktiv

## 9. Unterstützung

Wir unterstützen die Kundin bei Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Herausgabe, Widerspruch): Anfragen an uns leiten wir innert 3 Arbeitstagen weiter und setzen Weisungen innert 5 Arbeitstagen um. Teilnehmende können ihre Daten in der App selbst exportieren und löschen. Wir unterstützen zudem bei Datenschutz-Folgenabschätzungen und Meldungen an Behörden.

## 10. Meldung von Verletzungen

Jede Verletzung der Datensicherheit melden wir der Kundin per E-Mail binnen 24 Stunden, nachdem wir davon erfahren haben, ohne vorherige Risikoabwägung. Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Daten und Personen, mögliche Folgen und getroffene oder vorgeschlagene Massnahmen (Vorlage nach Leitfaden des EDÖB). Die Meldung an den EDÖB (Art. 24 revDSG) bzw. an die Aufsichtsbehörde binnen 72 Stunden (Art. 33 DSGVO) obliegt der Kundin.

## 11. Aufbewahrung und Löschung

Am 31. Januar nach der Saison löschen wir die Daten der Runde automatisch; 14 Tage vorher erhält die Kundin eine Erinnerung mit Exportmöglichkeit (Liste der Teilnehmenden, ohne Fragebogen-Antworten). Nach Wahl der Kundin geben wir die Daten bei Vertragsende vorher heraus (Export) oder löschen sie; gesetzliche Aufbewahrungspflichten bleiben vorbehalten. Es gilt folgende Tabelle:

Aufbewahrung und Löschung

Daten · Ort · Aufbewahrung · Löschung

Einladungen ohne Antwort (eingeladen, weder dabei noch abgesagt) · D1 · bis J + 1 Tag · J + 1 Tag, automatischer Job purge-unjoined; danach Nicht-Teilnehmende nur noch als Anzahl

Abgesagte Einladung («Nein, danke») · D1 · Name und Daten: keine; gesalzener E-Mail-Hash nur für diese Runde · Daten sofort; Hash am 31.1.

Profil der Teilnehmenden (Name, Arbeits-E-Mail, Fragebogen, Hinweistext) · D1 · bis Saisonende · 31.1. automatischer Job; zudem jederzeit auf Anfrage an hallo@wichtli.ch

Auslosung/Paare · D1 · bis Saisonende · 31.1.

Inhalt der Nachrichten und Hinweise (anonymer Chat) · D1 · bis Saisonende; gemeldete Nachrichten und Hinweise inkl. Absenderidentität als Beweismittel bis 90 Tage nach der Meldung · 31.1. (gemeldet: +90 Tage)

Wohnadresse aus dem Start (freiwillig, verschlüsselt) · D1 · bis Saisonende · 31.1. automatischer Job, beim Austritt sofort; entschlüsselt nur für den Versandexport

Lieferadresse (verschlüsselt) · D1 · von der Eingabe bis zur bestätigten Lieferung · 14 Tage nach der Lieferung (ohne Zustellmeldung: 30 Tage nach dem Versand), 14 Tage nach einer fehlgeschlagenen oder gutgeschriebenen Bestellung, spätestens 31.1.; entschlüsselt nur für den Versandexport

Personalisierte GIFs und Karten · D1 (Datei: R2 EU, sobald aktiv) · bis Saisonende; früher, wenn Absender oder Empfänger austritt · 31.1.

Fotowand: Fotos, Bildtexte und Herzen · D1 (Bilder: R2 EU, sobald aktiv) · bis Saisonende; früher, wenn die Person das Foto löscht oder austritt; gemeldete Fotos inkl. Identität der Person als Beweismittel bis 90 Tage nach der Meldung, ausser die Meldung wird verworfen · 31.1. (gemeldet: +90 Tage)

Paar-Gedächtnis fürs zweite Jahr (HMAC mit firmeneigenem Schlüssel; nur wenn die Firma es wählt) · D1 · bis zur nächsten Runde, max. 13 Monate · nach 13 Monaten, bei Kündigung des Abos oder der Verlängerung oder auf Löschwunsch der Person

Firmenkonto (Name und E-Mail der Admins) · D1 · solange die Kundenbeziehung besteht · auf Verlangen; nach 24 Monaten Inaktivität gelöscht

«Für 2027 vormerken» (Double-Opt-in-E-Mail + Zeitstempel) · D1 · bis 31.10.2027 · 31.10.2027 oder bei Abmeldung

Rechnungen, Stripe-Zahlungsdaten, Bestelldaten · Stripe + D1 · 10 Jahre gesetzlich (Art. 958f OR) · nach 10 Jahren

Sicherheits- und Zugriffslogs (ohne Inhalte) · Workers-Logs · 30 Tage · laufend

Protokoll der Adress-Entschlüsselungen (wer/wann, ohne Adresse) · D1 · 12 Monate · laufend

Protokoll der Datenschutzverletzungen · intern · 2 Jahre ab Meldung · danach gelöscht

Backups/Time Travel · D1 · bis 30 Tage · verfallen automatisch

J = Anmeldeschluss der Runde. Saisonende ist der 31. Januar. Aggregierte Zahlen ohne Personenbezug (z. B. Anzahl Teilnehmende pro Runde) dürfen bleiben.

## 12. Audit

Die Kundin kann die Einhaltung dieses AVV einmal pro Jahr anhand von Unterlagen prüfen, auf eigene Kosten. Wir stellen die nötigen Informationen bereit. Reichen die Unterlagen nicht aus oder verlangt eine Aufsichtsbehörde es, sind Prüfungen einschliesslich Inspektionen durch die Kundin oder eine von ihr beauftragte, zur Vertraulichkeit verpflichtete Prüferin möglich, mit 30 Tagen Vorankündigung, während der Geschäftszeiten und auf Kosten der Kundin.

## 13. Auslandstransfers

Die Daten werden in der EU gespeichert. Transfers in die USA erfolgen nur an Unterauftragsbearbeiter, die unter dem Data Privacy Framework (EU-US und Swiss-US) zertifiziert sind, zusätzlich abgesichert durch Standardvertragsklauseln. Kontakt: privacy@wichtli.ch.