

Auftragsverarbeitungsvertrag (AVV)

Zuletzt aktualisiert am 1. Mai 2026 · Vertrag nach Art. 28 DSGVO.

Dies ist eine Übersetzung, die nur zur Information dient. Bei Abweichungen zwischen dieser Übersetzung und der englischen Fassung ist die englische Fassung maßgeblich.

So funktioniert es

Dieser AVV ist Teil der Nutzungsbedingungen. Er wird automatisch wirksam, sobald ein Workspace angelegt wird und personenbezogene Daten darin gespeichert werden. Die Kundenorganisation, der der Workspace gehört, ist der Verantwortliche; Dazr ist der Auftragsverarbeiter. Eine Unterschrift ist nicht erforderlich; wenn Ihr Einkaufsprozess ein gegengezeichnetes Exemplar verlangt, schreiben Sie an legal@dazr.eu.

1. Begriffsbestimmungen

Begriffe in diesem AVV haben die Bedeutung, die ihnen die Verordnung (EU) 2016/679 (DSGVO) gibt. „Personenbezogene Kundendaten“ sind personenbezogene Daten, die der Verantwortliche (oder die in seinem Auftrag handelnden Mitglieder und Auditoren) in den Workspace einstellt, einschließlich personenbezogener Daten in Kontrollaufgaben, Nachweisen, Kommentaren, Dateien, Risiken, Vorfällen, Lieferantendatensätzen, Mitgliedern und Einladungen, Einsendungen über das öffentliche Meldeportal und im Aktivitätsprotokoll.

2. Gegenstand, Dauer, Art und Zweck

- Gegenstand: die Verarbeitung personenbezogener Kundendaten, damit der Verantwortliche sein Compliance-Programm für Informationssicherheit und Datenschutz über die Plattform Dazr Compliance führen kann.
- Dauer: die Laufzeit des Abonnements des Verantwortlichen zuzüglich der Übergangsfrist nach Vertragsende gemäß den Nutzungsbedingungen.
- Art und Zweck: Hosting, Speicherung, Übermittlung, Abruf, Löschung sowie die in den Nutzungsbedingungen und der Datenschutzerklärung beschriebenen Vorgänge.
- Art der personenbezogenen Daten: Identifikationsdaten der Workspace-Mitglieder und eingeladenen Auditoren (E-Mail-Adresse, Name, Rolle); gegebenenfalls Identifikationsdaten von Personen, die über das öffentliche Meldeportal oder als Hinweisgebende Vorfälle melden; Kontaktdaten von Arbeitgebern und betriebliche Metadaten, die der Verantwortliche hochlädt. Der Verantwortliche stellt sicher, dass er besondere Kategorien personenbezogener Daten nur hochlädt, wenn seine eigene Rechtsgrundlage dies erlaubt.
- Kategorien betroffener Personen: Beschäftigte, Auftragnehmer und eingeladene externe Auditoren des Verantwortlichen sowie alle Personen, die in Compliance-Inhalten genannt werden, die der Verantwortliche hochlädt.

3. Pflichten des Auftragsverarbeiters

1. Wir verarbeiten personenbezogene Kundendaten nur auf dokumentierte Weisung des Verantwortlichen. Die Weisungen bestehen in der Nutzung der vorgesehenen Funktionen der Plattform; sind wir der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt, informieren wir den Verantwortlichen.
2. Wir gewährleisten, dass sich die zur Verarbeitung personenbezogener Kundendaten befugten Personen zur Vertraulichkeit verpflichtet haben.
3. Wir ergreifen alle nach Art. 32 DSGVO (Sicherheit der Verarbeitung) erforderlichen Maßnahmen. Die aktuellen Maßnahmen sind in Abschnitt 7 beschrieben.
4. Wir halten die Bedingungen des Art. 28 Abs. 2 und 4 für die Inanspruchnahme von Unterauftragsverarbeitern

ein (siehe Abschnitt 6).

5. Unter Berücksichtigung der Art der Verarbeitung und der uns vorliegenden Informationen unterstützen wir den Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen, bei Meldungen von Datenschutzverletzungen, bei Datenschutz-Folgenabschätzungen und bei der vorherigen Konsultation der Aufsichtsbehörden (Art. 28 Abs. 3 lit. e und f).
6. Nach Abschluss der Leistungen löschen wir nach Wahl des Verantwortlichen alle personenbezogenen Kundendaten oder geben sie zurück und löschen vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Speicherpflicht besteht.
7. Wir stellen dem Verantwortlichen alle Informationen zum Nachweis der Einhaltung von Art. 28 zur Verfügung und ermöglichen Überprüfungen einschließlich Inspektionen und tragen dazu bei (siehe Abschnitt 9).

4. Pflichten des Verantwortlichen

- Der Verantwortliche sichert zu, dass er für die personenbezogenen Daten, die er in den Workspace einstellt, eine Rechtsgrundlage nach Art. 6 (und gegebenenfalls Art. 9) hat.
- Der Verantwortliche ist für die Richtigkeit der personenbezogenen Kundendaten und für die Beantwortung von Anträgen betroffener Personen zu seinem Workspace zuständig (Anträge, die bei uns eingehen, leiten wir an den Verantwortlichen weiter und unterstützen ihn nach Art. 28 Abs. 3 lit. e).
- Der Verantwortliche steuert den Zugriff (Rollen der Mitglieder, Einladungen von Auditoren, das öffentliche Meldeportal) über die Einstellungen der Plattform.

5. Internationale Übermittlungen

Personenbezogene Kundendaten werden standardmäßig in der Europäischen Union gespeichert. Hat ein Unterauftragsverarbeiter seinen Hauptsitz außerhalb der EU, gelten für Übermittlungen die Standardvertragsklauseln der Europäischen Kommission (Beschluss 2021/914), Modul 3 (Auftragsverarbeiter an Auftragsverarbeiter), mit den in Abschnitt 7 beschriebenen ergänzenden Maßnahmen. Die aktuellen Unterauftragsverarbeiter und ihre Standorte stehen unter </legal/subprocessors>.

6. Unterauftragsverarbeiter

1. Der Verantwortliche erlaubt uns, zur Erbringung des Dienstes Unterauftragsverarbeiter einzusetzen. Die aktuelle Liste steht unter </legal/subprocessors>.
2. Über beabsichtigte Hinzufügungen oder Ersetzungen informieren wir den Verantwortlichen mindestens 30 Tage im Voraus über das E-Mail-Abonnement auf dieser Seite oder per E-Mail an den Workspace-Eigentümer.
3. Der Verantwortliche kann aus berechtigten Datenschutzgründen widersprechen. Können wir dem Widerspruch nicht abhelfen, kann der Verantwortliche den betroffenen Dienst kündigen und erhält eine anteilige Erstattung für den nicht genutzten Rest des laufenden Abrechnungszeitraums.
4. Wir verpflichten jeden Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die nicht weniger schützen als die dieses AVV, und haften gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Unterauftragsverarbeiters.

7. Sicherheitsmaßnahmen (Art. 32)

- Verschlüsselung. Personenbezogene Kundendaten werden im Ruhezustand auf Anwendungsebene mit AES-256-GCM verschlüsselt, zusätzlich zur Verschlüsselung des Speicheranbieters. Jede Übertragung erfolgt über HTTPS mit HSTS-Preload, ohne unverschlüsselten Rückfall. Die Schlüssel werden per HKDF aus einem Hauptschlüssel abgeleitet, der nur in Umgebungsvariablen der Produktionsinfrastruktur liegt.
- Zugriffskontrolle. Rollenbasierte Zugriffskontrolle in der Plattform (Eigentümer, Admin, Mitglied, Auditor);

zeitlich begrenzte und widerrufbare Auditor-Sitzungen. Betrieblicher Zugriff ist auf ein kleines Support-Team über das Support-Portal beschränkt, das bewusst nur Metadaten zeigt.

- Authentifizierung. Passwortlose Anmeldung mit Einmalcode. HMAC-signierte Sitzungstoken mit begrenzter Gültigkeit. Ratenbegrenzung an jedem öffentlichen Endpunkt, auch bei der Admin-Anmeldung.
- Belastbarkeit und Integrität. Nur anhängbares Aktivitätsprotokoll jeder zustandsändernden Aktion. Backups innerhalb der EU. Die Integrität gespeicherter Daten wird über AEAD-Authentifizierungs-Tags geprüft; manipulierte Chiffretexte führen zu einem Fehler und werden nicht ausgeliefert.
- Netzwerk und Header. Strikte Content-Security-Policy mit einer Positivliste gehashter Inline-Skripte, strikte X-Frame-Options, X-Content-Type-Options nosniff und HSTS-Preload.
- Schwachstellenmanagement. Abhängigkeiten sind auf feste Versionen gesetzt; wir verfolgen Sicherheitshinweise und spielen Patches nach einem dem Schweregrad angemessenen Zeitplan ein.

8. Verletzung des Schutzes personenbezogener Daten

Werden wir auf eine Verletzung des Schutzes personenbezogener Kundendaten aufmerksam, benachrichtigen wir den Workspace-Eigentümer unverzüglich und spätestens 72 Stunden, nachdem wir davon Kenntnis erlangt haben (Art. 33 Abs. 2). Die Meldung beschreibt, soweit bekannt, die Art der Verletzung, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Maßnahmen und eine Anlaufstelle für weitere Informationen. Wir unterstützen den Verantwortlichen bei seinen eigenen Meldepflichten nach Art. 33 und Art. 34.

9. Überprüfungen

Der Verantwortliche (oder ein von ihm beauftragter externer Prüfer) kann die Einhaltung dieses AVV einmal in zwölf Monaten überprüfen, mit einer schriftlichen Ankündigung von mindestens 30 Tagen und während der Geschäftszeiten, in einer Weise, die unseren Betrieb nicht unangemessen beeinträchtigt und die Vertraulichkeit der Daten anderer Kunden wahrt. Für Überprüfungen über diesen Umfang hinaus können wir eine angemessene Vergütung verlangen. Kann eine Prüfpflicht nach Art. 28 Abs. 3 lit. h durch eine Bescheinigung eines Dritten erfüllt werden, die uns vorliegt, stellen wir diese anstelle einer Vor-Ort-Prüfung bereit.

10. Haftung

Die Haftung jeder Partei aus diesem AVV unterliegt den Begrenzungen der Nutzungsbedingungen. Diese Begrenzungen beschränken nicht die Haftung für Schäden, die betroffenen Personen nach Art. 82 DSGVO entstehen.

11. Laufzeit und Beendigung

Dieser AVV gilt, solange wir personenbezogene Kundendaten verarbeiten, und bleibt nach Beendigung der Nutzungsbedingungen in dem Umfang und für die Dauer wirksam, in der wir noch solche Daten besitzen. Die Abschnitte 8 (Verletzungen), 9 (Überprüfungen) und 12 (Rückgabe und Löschung) gelten über die Beendigung hinaus.

12. Rückgabe und Löschung

Nach Beendigung des Dienstes kann der Verantwortliche die Workspace-Daten während der 30-tägigen Übergangsfrist aus den Nutzungsbedingungen mit den Exportfunktionen der Plattform exportieren. Nach Ablauf der Frist löschen wir die personenbezogenen Kundendaten; Backups laufen gemäß unseren Aufbewahrungsfristen aus. Daten, die wir aufbewahren müssen (z. B. Rechnungen nach italienischem Handelsrecht), bewahren wir nur für die Dauer dieser Pflicht auf.

13. Rangfolge

Bei Widersprüchen zwischen diesem AVV und den Nutzungsbedingungen oder der Datenschutzerklärung hat dieser AVV in Fragen der Datenverarbeitung Vorrang. Für Übermittlungen außerhalb der EU vereinbarte Standardvertragsklauseln haben in den von ihnen geregelten Fragen Vorrang vor diesem AVV und den Nutzungsbedingungen.

14. Mitteilungen

- An Dazr: privacy@dazr.eu (Datenschutz) oder security@dazr.eu (Vorfälle).
- An den Verantwortlichen: die zum Zeitpunkt der Mitteilung hinterlegte E-Mail-Adresse des Workspace-Eigentümers.