chrondo

Auftragsverarbeitungsvertrag

Stand: 21. Juli 2026

Dieser Auftragsverarbeitungsvertrag (nachfolgend "AVV") gilt zwischen der **PROGEEK GmbH** (nachfolgend "Anbieter") als Auftragsverarbeiter und dem Kunden (nachfolgend "Verantwortlicher" oder "Kunde") und ist Bestandteil des zwischen den Parteien auf Grundlage der Allgemeinen Geschäftsbedingungen (AGB) geschlossenen Vertrags über die Nutzung der Zeiterfassungslösung Chrondo (nachfolgend "Nutzungsvertrag"). Maßgeblich für ein konkretes Vertragsverhältnis ist die bei Vertragsschluss gültige, unter chrondo.de/avv veröffentlichte Fassung; sie ist am oben angegebenen Stand-Datum erkennbar.

§ 1 Gegenstand und Dauer der Verarbeitung

Der Auftragsverarbeiter (PROGEEK GmbH, nachfolgend "Anbieter") verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen (nachfolgend "Kunde") im Rahmen der Bereitstellung der Zeiterfassungslösung Chrondo gemäß dem Nutzungsvertrag.

Die Dauer der Verarbeitung entspricht der Laufzeit des Nutzungsvertrags. Nach Beendigung des Nutzungsvertrags gelten die Regelungen in § 10 (Löschung und Rückgabe von Daten) dieses AVV.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung dient der Bereitstellung der SaaS-Lösung Chrondo zur digitalen Zeiterfassung. Dies umfasst insbesondere:

- Erfassung und Speicherung von Arbeitszeiten
- Erfassung und Verwaltung von Abwesenheiten (Urlaub, Krankheit, etc.)
- Verwaltung von Mitarbeiterkonten und Zugangsdaten
- Authentifizierung von Nutzern via NFC-Chip/Karte oder Mobile App
- Bereitstellung von Auswertungen und Übersichten für den Kunden

§ 3 Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten werden verarbeitet:

- Stammdaten: Name, Vorname, Personalnummer (sofern vergeben)
- Kontaktdaten: E-Mail-Adresse (sofern für Login erforderlich)
- Beschäftigungsdaten: Abteilung, Standort, Arbeitszeitmodell
- Zeiterfassungsdaten: Kommen-/Gehen-Zeiten, Pausenzeiten, Überstunden
- Abwesenheitsdaten: Urlaubstage, Krankheitstage, sonstige Abwesenheiten
- Technische Daten: NFC-Chip-ID, App-Login-Daten, IP-Adressen bei Zugriff

Soweit der Kunde Abwesenheiten mit der Abwesenheitsart "Krankheit" erfasst, werden Gesundheitsdaten und damit besondere Kategorien personenbezogener Daten im Sinne des Art. 9

DSGVO verarbeitet. Für diese Daten gelten eine strikte Zweckbindung, restriktive Zugriffsbeschränkungen über das Rollen- und Berechtigungskonzept sowie ein Verbot der Weitergabe an Dritte. Erfasst wird ausschließlich die Tatsache und Dauer der Abwesenheit, keine Diagnosen oder sonstigen medizinischen Angaben. Der Kunde bleibt dafür verantwortlich, dass für die Verarbeitung eine geeignete Rechtsgrundlage besteht (insbesondere Art. 9 Abs. 2 lit. b DSGVO i. V. m. § 26 Abs. 3 BDSG).

§ 4 Kategorien betroffener Personen

Betroffen sind die Mitarbeiter und Beschäftigten des Kunden, deren Arbeitszeiten über Chrondo erfasst werden.

§ 5 Pflichten des Anbieters

Der Anbieter verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Kunden. Der Nutzungsvertrag (einschließlich der AGB) und dieser AVV stellen die allgemeine Weisung dar. Weitergehende Weisungen bedürfen der Textform.

Weisungsberechtigt sind die vom Kunden benannten Ansprechpartner bzw. Administratoren. Der Kunde teilt dem Anbieter Änderungen des Kreises der weisungsberechtigten Personen unverzüglich in Textform mit.

Der Anbieter gewährleistet, dass die mit der Verarbeitung betrauten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Anbieter unterstützt den Kunden bei der Einhaltung der Pflichten gemäß Art. 32–36 DSGVO (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung), soweit dies unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen möglich ist.

Der Anbieter informiert den Kunden ohne unangemessene Verzögerung gemäß Art. 33 Abs. 2 DSGVO, sobald er Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangt, spätestens jedoch innerhalb von 48 Stunden nach gesicherter Kenntniserlangung; bei Vorfällen, deren Eintritt oder Ausmaß zunächst unklar ist, beginnt die Frist mit der gesicherten Bestätigung der Verletzung. Soweit die vollständigen Angaben nicht innerhalb dieser Frist verfügbar sind, erfolgt eine Erstmeldung mit den verfügbaren Informationen; weitere Informationen werden unverzüglich nachgereicht. Die Meldung enthält mindestens:

- Art der Verletzung
- Betroffene Datenkategorien und ungefähre Anzahl betroffener Personen
- Wahrscheinliche Folgen
- Ergriffene oder vorgeschlagene Maßnahmen

Der Anbieter informiert den Kunden, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt.

§ 6 Technische und organisatorische Maßnahmen (TOM)

Der Anbieter trifft die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Diese Maßnahmen sind Bestandteil des AVV und entsprechen dem Stand der Technik. Der Anbieter ist berechtigt, einzelne Maßnahmen weiterzuentwickeln, sofern das Schutzniveau nicht unterschritten wird.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Physische Zutrittskontrolle zum Rechenzentrum durch den Hosting-Dienstleister (zertifiziert nach ISO 27001)
- Zugangskontrolle: Authentifizierung mit individuellen Zugangsdaten, Passwortrichtlinien (Mindestlänge 12 Zeichen, Komplexitätsanforderungen), automatische Sperrung nach mehrfachen Fehlversuchen
- Zugriffskontrolle: Rollenbasiertes Berechtigungskonzept (Need-to-know-Prinzip), regelmäßige Berechtigungsreviews
- Administrative Zugriffe: Wartungs- und Administrationszugriffe ausschließlich über gesicherte, verschlüsselte Verbindungen, beschränkt auf einen kleinen Kreis berechtigter Mitarbeiter
- Trennungskontrolle: Mandantentrennung auf Datenbankebene; Trennung von Entwicklungs-, Test- und Produktionsumgebungen; in Test- und Entwicklungsumgebungen werden keine produktiven personenbezogenen Daten verwendet
- Verschlüsselung in Transit: TLS 1.3 als Standard, mindestens TLS 1.2 als Fallback (HTTPS); für sämtliche Datenübertragungen, entsprechend BSI TR-02102-2
- Verschlüsselung at rest: Datenbank- und Backup-Verschlüsselung mit AES-256

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Eingabekontrolle: Protokollierung sicherheitsrelevanter Datenänderungen mit Zeitstempel und Nutzerkennung; Aufbewahrung der Logs für mindestens 90 Tage
- Weitergabekontrolle: Ausschließlich verschlüsselte Übertragungswege; keine unverschlüsselte Übertragung personenbezogener Daten per E-Mail

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Backup-Konzept: Tägliche, automatisierte Datensicherungen mit einer Aufbewahrung von 30 Tagen
- Recovery: Definierte Wiederherstellungsverfahren mit RTO ≤ 24 Stunden und RPO ≤ 24 Stunden
- Monitoring: Automatisierte Überwachung der Systemverfügbarkeit mit Alarmierung des Betriebsteams bei Störungen
- Redundanz: Redundante Serverinfrastruktur beim Hosting-Dienstleister
- Patch-Management: Einspielung sicherheitsrelevanter Updates innerhalb angemessener Frist nach Verfügbarkeit (kritische Patches in der Regel innerhalb von 14 Tagen)

Regelmäßige Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Mindestens jährliche Überprüfung und Aktualisierung der TOM
- Auftrags- bzw. Datenschutzkontrolle: Verpflichtung der Mitarbeiter auf Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO)
- Vier-Augen-Prinzip: Verbindliche Code-Reviews für Änderungen am produktiven System
- Incident-Response-Prozess: Dokumentierter Prozess zur Behandlung von Sicherheitsvorfällen

§ 7 Unterauftragsverarbeitung

Der Kunde erteilt dem Anbieter eine allgemeine Genehmigung zur Einschaltung von Unterauftragsverarbeitern. Der Anbieter informiert den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mit einer Frist von 30 Tagen vor der Änderung.

Der Kunde kann gegen die beabsichtigte Änderung innerhalb von 14 Tagen nach Mitteilung Einspruch erheben. Im Falle eines berechtigten Einspruchs bemüht sich der Anbieter um eine alternative Lösung. Kann keine Einigung erzielt werden, steht dem Kunden ein außerordentliches Kündigungsrecht zu.

Der Anbieter stellt sicher, dass Unterauftragsverarbeiter vertraglich mindestens denselben Datenschutzpflichten unterworfen werden, wie sie in diesem AVV festgelegt sind.

Aktuelle Unterauftragsverarbeiter:

Dienstleister	Zweck	Serverstandort
DigitalOcean, LLC, 101 Avenue of the Americas, 10th Floor, New York, NY 10013, USA	Hosting / Serverinfrastruktur	Deutschland (Frankfurt am Main)

Die Speicherung und Verarbeitung der personenbezogenen Daten erfolgt ausschließlich in Rechenzentren in Deutschland (Frankfurt am Main). Da DigitalOcean, LLC ein Unternehmen mit Sitz in den USA ist, kann ein Zugriff aus einem Drittland im Sinne der DSGVO nicht vollständig ausgeschlossen werden. DigitalOcean ist nach dem EU-US Data Privacy Framework (DPF) zertifiziert; ergänzend bestehen mit DigitalOcean EU-Standardvertragsklauseln gemäß Art. 46 DSGVO (Beschluss (EU) 2021/914). Die Mobile Apps des Anbieters nutzen keine Push-Notification-Dienste (insbesondere weder Apple APNs noch Google FCM) und auch keine sonstigen Dienste, die eine darüber hinausgehende Übermittlung personenbezogener Daten in Drittländer auslösen würden. Sollten zukünftig weitere Übermittlungen in Drittländer erforderlich werden, wird der Anbieter den Kunden gemäß § 7 Abs. 1 vorab informieren und die Übermittlung durch geeignete Garantien gemäß Art. 46 DSGVO absichern; auf Anfrage des Kunden wird eine Transfer Impact Assessment (TIA) zur Verfügung gestellt.

§ 8 Rechte der betroffenen Personen

Der Anbieter unterstützt den Kunden nach Möglichkeit bei der Erfüllung von Betroffenenrechten (Art. 15–22 DSGVO), insbesondere bei Auskunfts-, Berichtigungs-, Löschungs- und Übertragbarkeitsanfragen.

Richtet eine betroffene Person ein Ersuchen direkt an den Anbieter, leitet dieser das Ersuchen unverzüglich an den Kunden weiter und wartet dessen Weisung ab, sofern der betroffenen Person nicht offensichtlich eine Antwort erteilt werden kann.

Anfragen zum Datenschutz können an info@progeek.de gerichtet werden.

§ 9 Kontrollrechte des Kunden

Der Kunde hat das Recht, die Einhaltung der in diesem AVV festgelegten Pflichten zu überprüfen. Der Anbieter stellt dem Kunden hierfür die erforderlichen Informationen zur Verfügung.

Überprüfungen und Inspektionen sind nach vorheriger schriftlicher Ankündigung mit einer Frist von mindestens vier Wochen, höchstens einmal jährlich und unter Beachtung der betrieblichen Abläufe möglich, sofern keine konkreten Anhaltspunkte für einen Datenschutzverstoß vorliegen. Der Anbieter kann anstelle einer Vor-Ort-Prüfung auch aktuelle Zertifikate, Berichte unabhängiger Prüfer oder andere geeignete Nachweise vorlegen. Der angemessene Aufwand des Anbieters für

die Unterstützung außerordentlicher Audits oder zusätzlicher Prüfungen über die jährliche Routine hinaus wird als erweiterter Support gemäß § 8.2 der AGB nach Aufwand berechnet.

§ 10 Löschung und Rückgabe von Daten

Nach Beendigung des Nutzungsvertrags stellt der Anbieter dem Kunden die gespeicherten personenbezogenen Daten gemäß § 15 der AGB in einem gängigen, maschinenlesbaren Format (CSV oder JSON) bereit.

Nach Ablauf der Herausgabefrist (30 Tage nach Vertragsende) löscht der Anbieter sämtliche im Auftrag verarbeiteten personenbezogenen Daten unwiderruflich, sofern nicht gesetzliche Aufbewahrungspflichten entgegenstehen.

Der Anbieter bestätigt die vollständige Löschung auf Anfrage des Kunden in Textform.

§ 11 Verstöße und Beendigung

Verstößt der Anbieter gegen seine Pflichten aus diesem AVV oder verarbeitet er personenbezogene Daten weisungswidrig, kann der Kunde den Anbieter anweisen, die betroffene Verarbeitung auszusetzen, bis der Verstoß behoben ist.

Der Kunde ist berechtigt, den Nutzungsvertrag außerordentlich zu kündigen, wenn der Anbieter wesentlich oder fortdauernd gegen diesen AVV verstößt und den Verstoß trotz angemessener Fristsetzung nicht abstellt, oder wenn eine bindende Entscheidung einer zuständigen Aufsichtsbehörde oder eines Gerichts die weitere Verarbeitung untersagt.

Im Falle der Beendigung gelten die Regelungen zur Löschung und Rückgabe von Daten (§ 10) entsprechend.

§ 12 Schlussbestimmungen

Dieser AVV ist Bestandteil des Nutzungsvertrags und tritt mit dessen Zustandekommen in Kraft.

Bei Widersprüchen zwischen diesem AVV und den AGB gehen die Regelungen dieses AVV in datenschutzrechtlichen Fragen vor.

Für die Haftung der Parteien gelten die Regelungen des Nutzungsvertrags (§ 17 der AGB). Die zwingende gesetzliche Haftung, insbesondere die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO, bleibt unberührt.

Änderungen dieses AVV bedürfen der Textform.