Dayklar

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Version 1.6 · Stand 13.11.2026

zwischen der Firma, die diesen Vertrag in Dayklar abschließt („Auftraggeber“), und Oliver Riedmüller, Dayklar, Riedlinger Straße 18, 88400 Biberach an der Riß („Auftragnehmer“).

1. Gegenstand und Dauer

Der Auftragnehmer stellt dem Auftraggeber die Aufgaben-App Dayklar bereit und verarbeitet dabei personenbezogene Daten in dessen Auftrag. Grundlage sind die AGB von Dayklar. Dieser Vertrag gilt, solange der Auftragnehmer Daten für den Auftraggeber verarbeitet.

2. Art, Zweck und Umfang

- Zweck: Bereitstellung von Dayklar für das Team des Auftraggebers, also Aufgaben, Projekte, Zuweisungen, Kalender, Erinnerungen, Anhänge, KI-Vorschläge auf Anforderung und Support.
- Arten von Daten: Namen, E-Mail-Adressen, Profilbilder und Rollen der Nutzer; Anmeldedaten (Passwort als Prüfwert, Zwei-Faktor, Sitzungen mit IP-Adresse und Browser); Inhalte wie Aufgaben, Notizen, Checklisten, Termine und Anhänge; Zeitzone und Arbeitszeiten; Nutzungsdaten wie letzte Aktivität; Einladungen und Benachrichtigungen; personenbezogene Daten Dritter, die Nutzer in Inhalte schreiben.
- Betroffene: Beschäftigte und Beauftragte des Auftraggebers, eingeladene Personen und Dritte, die in Inhalten genannt werden.
- Besondere Kategorien nach Art. 9 DSGVO sind nicht vorgesehen. Der Auftraggeber legt sie nur ab, wenn er die Zulässigkeit selbst geprüft hat.

3. Weisungen

Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, auch bei Übermittlungen in Drittländer, außer das Recht der EU oder eines Mitgliedstaats verpflichtet ihn dazu. Dann teilt er dem Auftraggeber diese Pflicht vorher mit, soweit das Recht das nicht verbietet. Weisungen sind dieser Vertrag, die Einstellungen, die der Auftraggeber in Dayklar wählt, und Weisungen in Textform, etwa per E-Mail. Hält der Auftragnehmer eine Weisung für rechtswidrig, sagt er das dem Auftraggeber unverzüglich.

4. Pflichten des Auftragnehmers

- Alle Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet.
- Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen aus Anlage 1 (Art. 32 DSGVO). Er darf sie weiterentwickeln, wenn das Schutzniveau nicht sinkt.

- Er unterstützt den Auftraggeber bei Anfragen von Betroffenen (Art. 12 bis 22 DSGVO), vor allem mit den Funktionen in Dayklar zum Berichtigen, Exportieren und Löschen, und leitet Anfragen, die bei ihm eingehen, unverzüglich weiter.
- Er unterstützt den Auftraggeber bei Sicherheit, Meldungen von Datenpannen, Datenschutz-Folgenabschätzung und vorheriger Konsultation (Art. 32 bis 36 DSGVO).
- Eine Verletzung des Schutzes der Daten meldet er dem Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt.
- Er stellt alle Informationen bereit, die zum Nachweis dieser Pflichten nötig sind, und ermöglicht Überprüfungen. Zuerst genügen schriftliche Auskünfte und Nachweise der Dienstleister. Prüfungen vor Ort sind nach Absprache mit einer Frist von vier Wochen möglich.
- Ein Datenschutzbeauftragter ist nicht benannt, weil keine Pflicht besteht. Ansprechpartner ist Oliver Riedmüller, datenschutz@dayklar.com.

5. Unterauftragsverarbeiter

- Der Auftraggeber genehmigt die Unterauftragsverarbeiter aus Anlage 2. Die aktuelle Liste steht unter dayklar.com/recht/unterauftragsverarbeiter.
- Einen neuen oder geänderten Unterauftragsverarbeiter kündigt der Auftragnehmer mindestens 30 Tage vorher per E-Mail an Inhaber und Admins an. Der Auftraggeber kann in dieser Zeit aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Findet sich keine Lösung, kann er den Vertrag über Dayklar zum Wirksamwerden der Änderung kündigen.
- Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten (Art. 28 Abs. 4 DSGVO). Übermittlungen in Drittländer stützen sich auf einen Angemessenheitsbeschluss oder auf Standardvertragsklauseln.
- Keine Unterauftragsverarbeiter sind Paddle, das als Verkäufer selbst verantwortlich ist, und reine Transportdienste wie die verschlüsselten Mitteilungsdienste der Browser.

6. Support-Zugriff

Der Auftragnehmer sieht Inhalte des Auftraggebers nur, wenn ein Nutzer den Support-Zugriff in Dayklar freigibt, für 24 Stunden oder 7 Tage. Jeder Zugriff wird protokolliert und lässt sich jederzeit beenden. Ohne Freigabe greift er nur zu, wenn es zur Abwehr einer Störung oder eines Angriffs nötig ist oder ein Gesetz es verlangt, und informiert dann den Auftraggeber.

7. Pflichten des Auftraggebers

Der Auftraggeber ist für die Zulässigkeit der Verarbeitung und die Information der Betroffenen verantwortlich. Er legt fest, wer im Team welche Rolle hat, und informiert den Auftragnehmer unverzüglich, wenn er Fehler in der Verarbeitung bemerkt.

8. Ende, Rückgabe und Löschung

Nach dem Ende des Vertrags kann der Auftraggeber seine Daten noch 30 Tage exportieren. Danach löscht der Auftragnehmer sie, in den Sicherungen nach Ablauf von 7 Tagen, außer ein Gesetz verlangt

die Aufbewahrung. Auf Wunsch bestätigt er die Löschung in Textform.

9. Haftung und Schlussbestimmungen

- Für die Haftung gegenüber Betroffenen gilt Art. 82 DSGVO. Im Verhältnis zwischen den Parteien gelten die Regeln zur Haftung aus den AGB von Dayklar, Fassung Firma.
- Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes den AGB vor.
- Änderungen dieses Vertrags kündigt der Auftragnehmer mindestens 6 Wochen vorher per E-Mail an, wie in den AGB beschrieben.
- Es gilt deutsches Recht. Gerichtsstand ist Biberach an der Riß, soweit gesetzlich zulässig.

Abgeschlossen in Dayklar durch [Name] für [Firmenname] am [Datum].

Anlage 1: Technische und organisatorische Maßnahmen (folgt)
Anlage 2: Unterauftragsverarbeiter (siehe Seite „Unterauftragsverarbeiter“)

Anlage 1: Technische und organisatorische Maßnahmen

Stand 13.11.2026. Die Maßnahmen beschreiben, wie Dayklar tatsächlich gebaut ist.

1. Vertraulichkeit

- Rechenzentren: Dayklar betreibt keine eigenen Server. Anwendung bei Vercel (Funktionen in Frankfurt am Main), Datenbank bei Neon in Frankfurt am Main, Dateien bei Cloudflare R2 mit Speicherort EU, KI über das KI-Gateway von Vercel mit Eingang und Verarbeitung in der EU. Den physischen Schutz der Rechenzentren übernehmen diese Anbieter, Nachweise wie SOC 2 und ISO 27001 liegen dort vor.
- Anmeldung: Passwörter nur als Prüfwert mit scrypt. Anmeldelinks gelten 15 Minuten und einmal und liegen nur als Prüfwert vor. Zwei-Faktor mit App und 10 Wiederherstellungscodes, für eine Firma als Pflicht einschaltbar. Nach 5 falschen Passwörtern 15 Minuten Sperre, dazu eine Bremse je IP-Adresse. Sitzungen enden nach 30 Tagen ohne Nutzung und lassen sich in den Einstellungen einzeln oder alle beenden.
- Rechte: Rollen Inhaber, Admin und Mitglied. Jede Abfrage ist auf Nutzer und Firma beschränkt. Geheime Links (Einladungen, Kalender-Abo, Bildschirm-Kopplung) liegen nur als Prüfwert vor. Dateien gibt es nur über kurzlebige, signierte Links.
- Betreiber-Konsole: Zugang nur für freigegebene Konten, immer mit Zwei-Faktor, mit eigenem Cookie für 12 Stunden, gebunden an die Sitzung. Rollen mit getrennten Rechten (Superadmin, Support, Finanzen, Marketing). Inhalte von Kunden zeigt die Konsole nur mit Support-Freigabe, befristet und protokolliert.
- Konten bei Dienstleistern: Zugang nur mit Passkey oder Zwei-Faktor: GitHub und Sentry mit Passkey, Vercel und Neon über die Anmeldung mit GitHub, Cloudflare, Resend, IONOS und Paddle mit Zwei-Faktor. Schlüssel liegen nur in den geschützten Umgebungsvariablen von Vercel, nie im Code.
- Trennung: Logische Trennung der Kunden über Firmen- und Nutzer-ID. Entwicklung und Tests mit eigener Datenbank ohne echte Daten, Bezahlung im Test mit Paddles Testumgebung.
- Verschlüsselung: Übertragung nur über HTTPS mit HSTS für zwei Jahre, auch für Subdomains. Speicherung verschlüsselt bei Neon, Cloudflare und Vercel. Mitteilungen Ende-zu-Ende verschlüsselt. Fehlermeldungen ohne Inhalte, Namen, E-Mail- und IP-Adressen.

2. Integrität

- Weitergabe: Nur über verschlüsselte Verbindungen, keine Datenträger. An die KI gehen nur die nötigen Felder, Exporte startet nur der Nutzer selbst.
- Nachvollziehbarkeit: Protokoll der Verwaltungsschritte je Firma, Protokoll der Betreiber-Konsole, Protokoll jedes Support-Zugriffs, Zeitstempel für Anlegen und Ändern.
- Schutz der Anwendung: Sicherheits-Kopfzeilen gegen Einbetten und Auspähen, Schutz vor Abrufen ins interne Netz beim Laden fremder Kalender (nur öffentliche Adressen, Zeit- und Größenlimit), Größenlimits für Dateien. Jede Änderung durchläuft vor dem Live-Gang eine automatische Prüfung (Typen, Regeln, Build).

3. Verfügbarkeit und Belastbarkeit

- Hosting mit Ausfallsicherheit bei den Anbietern, Datenbank mit Wiederherstellung auf jeden Zeitpunkt der letzten 7 Tage.
- Jede Version lässt sich bei Vercel sofort zurückrollen.
- Statusseite status.dayklar.com, Fehlerüberwachung mit Sentry.
- Täglicher Aufräum-Job: Löschen nach Fristen, verwaiste Dateien, alte Codes und Meldungen.

4. Regelmäßige Überprüfung

- Diese Maßnahmen prüft Oliver mindestens einmal im Jahr und nach größeren Änderungen.
- Dienstleister werden vor dem Einsatz geprüft (Vertrag, Speicherort, Übermittlung), Änderungen ihrer Bedingungen verfolgt.
- Ablauf bei Datenpannen nach festem Notfallplan: erkennen, eindämmen, bewerten, Auftraggeber unverzüglich informieren, dokumentieren.
- Zugriffsrechte in der Konsole werden bei jeder Änderung im Betreiber-Team geprüft.

5. Organisation

- Zugriff auf Systeme und Daten hat nur Oliver Riedmüller. Weitere Personen erhalten Zugriff nur nach Verpflichtung auf Vertraulichkeit und nur mit den nötigen Rechten.
- Arbeitsgeräte mit verschlüsselter Festplatte, Bildschirmsperre und aktuellen Updates.
- Löschkonzept: Konten 30 Tage nach „Konto löschen“, Meldungen der Glocke nach 30 Tagen, Einladungen 30 Tage nach Annahme, Ablauf oder Zurückziehen, Zählungen falscher Passwörter nach einem Tag; abgelaufene Sitzungen und Anmeldelinks, ersetzte Logos und verwaiste Dateien täglich.

Anlage 2: Unterauftragsverarbeiter

Dienstleister, die Daten in unserem Auftrag verarbeiten · Stand 13.11.2026

Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA

Zweck: Hosting von Website und App

Ort: Frankfurt am Main; Bilder und Programmdateien auch aus Rechenzentren in deiner Nähe

Grundlage: Vertrag zur Auftragsverarbeitung mit Standardvertragsklauseln

Databricks, Inc. (Neon), USA

Zweck: Datenbank

Ort: Frankfurt am Main

Grundlage: Vertrag zur Auftragsverarbeitung mit Standardvertragsklauseln

Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA

Zweck: Dateiablage R2 für Anhänge, Profilbilder und Logos

Ort: EU

Grundlage: Vertrag zur Auftragsverarbeitung, Data Privacy Framework und Standardvertragsklauseln

Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA

Zweck: Versand von E-Mails

Ort: Versand aus Irland

Grundlage: Vertrag zur Auftragsverarbeitung, Data Privacy Framework und Standardvertragsklauseln

Vercel Inc. (KI-Gateway), 440 N Barranca Ave #4133, Covina, CA 91723, USA · KI

Zweck: KI-Vorschläge mit Claude Haiku 4.5, verarbeitet bei Amazon Bedrock (Amazon Web Services) über das Konto von Vercel, ohne Speicherung und ohne Training

Ort: EU: Eingang und Verarbeitung; technische Angaben ohne Inhalte (Zeitpunkt, Tokens, Kosten) in den USA

Grundlage: Vertrag zur Auftragsverarbeitung mit Standardvertragsklauseln; Amazon Web Services ist Unterauftragsverarbeiter von Vercel

Functional Software, Inc. (Sentry), 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA

Zweck: Fehlermeldungen ohne Inhalte, Namen, E-Mail- und IP-Adressen

Ort: Frankfurt am Main

Grundlage: Vertrag zur Auftragsverarbeitung, Data Privacy Framework und Standardvertragsklauseln

IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland

Zweck: Unser Postfach für E-Mails an hallo@dayklar.com, datenschutz@dayklar.com und barrierefreiheit@dayklar.com

Ort: EU

Grundlage: Vertrag zur Auftragsverarbeitung

Nicht in unserem Auftrag

- Paddle.com Market Limited, 30 Old Bailey, London EC4M 7AU, Vereinigtes Königreich: Verkäufer von Pro und Team und für die Zahlung selbst verantwortlich. Für das Vereinigte Königreich gilt ein Angemessenheitsbeschluss der EU-Kommission.
- Die Mitteilungsdienste der Browser-Hersteller (Google, Apple, Mozilla, Microsoft) transportieren Mitteilungen nur verschlüsselt und können sie nicht lesen.
- Google und Microsoft, wenn du dich dort anmeldest, als eigene Verantwortliche.