Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

zwischen dem Kunden (Betrieb, der Horella nutzt — nachfolgend **„Auftraggeber"**) und der

Mathonyx GmbH, Achterum 1, 26736 Krummhörn (nachfolgend **„Auftragnehmerin"**).

Dieser Vertrag ist Bestandteil des Nutzungsvertrags über die Software „Horella" (AGB, abrufbar unter /agb/). Er wird elektronisch geschlossen über die ausdrückliche Annahmeerklärung im Produkt mit versionierter Protokollierung (protokolliert werden Version, eingefrorene Fassung, Kunde, Benutzer, Zeitstempel und Prüfsumme der Fassung); das wahrt die Textform des Art. 28 Abs. 9 DSGVO.

1. Gegenstand und Dauer

1.1 Die Auftragnehmerin stellt die SaaS-Software Horella (Dienstplanung, Arbeitszeiterfassung, Abwesenheitsverwaltung, Auswertungen) bereit und verarbeitet dabei personenbezogene Daten im Auftrag des Auftraggebers.

1.2 Die Dauer dieses Vertrags entspricht der Laufzeit des Nutzungsvertrags. Ziffer 11 gilt über das Vertragsende hinaus.

2. Art und Zweck der Verarbeitung, Datenkategorien, betroffene Personen

Ergeben sich aus **Anlage 1**. Die Verarbeitung erfolgt an den in Anlage 3 bezeichneten Verarbeitungsorten. Die Kernanwendung wird im Europäischen Wirtschaftsraum betrieben. Eine Verarbeitung in einem Drittland erfolgt nur, wenn der betreffende Unterauftragsverarbeiter in Anlage 3 aufgeführt ist und die Voraussetzungen des Kapitels V DSGVO erfüllt sind.

3. Weisungsrecht des Auftraggebers

3.1 Die Auftragnehmerin verarbeitet die Daten ausschließlich nach dokumentierter Weisung des Auftraggebers. Die Nutzung der Software-Funktionen durch den Auftraggeber gilt als Weisung; darüber hinausgehende Weisungen erfolgen in Textform an support@horella.com.

3.2 Hält die Auftragnehmerin eine Weisung für datenschutzrechtlich unzulässig, informiert sie den Auftraggeber unverzüglich und setzt die Ausführung der betroffenen Weisung bis zur Klärung aus. Eine weiterhin rechtswidrige Weisung wird nicht ausgeführt. Können die Parteien keine rechtmäßige Lösung finden, kann die Auftragnehmerin die hiervon betroffene Verarbeitung aussetzen oder den betroffenen Vertragsteil aus wichtigem Grund beenden.

4. Pflichten der Auftragnehmerin

- a) Verarbeitung nur im Rahmen der Vereinbarung und der Weisungen (Art. 28 Abs. 3 lit. a);
- b) Vertraulichkeitsverpflichtung aller mit der Verarbeitung befassten Personen (Art. 28 Abs. 3 lit. b);
- c) Umsetzung und laufende Anpassung der technischen und organisatorischen Maßnahmen nach **Anlage 2** (Art. 32); Anpassungen sind zulässig, solange das Schutzniveau nicht unterschritten wird;
- d) Unterstützung des Auftraggebers nach Ziff. 7 und 8;
- e) Datenschutzrechtlicher Kontakt der Auftragnehmerin: datenschutz@horella.com oder support@horella.com. Soweit ein Datenschutzbeauftragter bestellt ist, werden dessen Kontaktdaten auf der Website veröffentlicht und dem Auftraggeber mitgeteilt;
- f) Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

5. Technische und organisatorische Maßnahmen

Die zum Vertragsschluss geltenden Maßnahmen sind in **Anlage 2** festgelegt. Die Auftragnehmerin überprüft sie regelmäßig und entwickelt sie am Stand der Technik weiter.

6. Unterauftragsverarbeiter

6.1 Der Auftraggeber erteilt die allgemeine Genehmigung zum Einsatz der in **Anlage 3** aufgeführten Unterauftragsverarbeiter.

6.2 Die Auftragnehmerin informiert den Auftraggeber mindestens 30 Tage vor der beabsichtigten Neuaufnahme oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann innerhalb dieser Frist aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Ist eine Lösung nicht möglich, darf die Auftragnehmerin den betreffenden Unterauftragsverarbeiter für die Daten des widersprechenden Auftraggebers erst einsetzen, nachdem der Auftraggeber den betroffenen Vertragsteil vor Beginn des Einsatzes kündigen konnte. Die Auftragnehmerin bleibt für die Einhaltung der Pflichten des Unterauftragsverarbeiters verantwortlich.

6.3 Mit jedem Unterauftragsverarbeiter werden Verpflichtungen vereinbart, die den Pflichten dieses Vertrags entsprechen. Bei Verarbeitung außerhalb des EWR stellt die Auftragnehmerin geeignete Garantien nach Kap. V DSGVO sicher (Anlage 3).

7. Unterstützung bei Betroffenenrechten

Die Auftragnehmerin unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei dessen Pflicht, Anträge auf Wahrnehmung von Betroffenenrechten (Art. 12–23 DSGVO) zu beantworten — insbesondere durch die in der Software vorhandenen Auskunfts-, Export-, Berichtigungs- und Löschfunktionen. Wendet sich eine betroffene

Person direkt an die Auftragnehmerin, leitet diese den Antrag unverzüglich an den Auftraggeber weiter.

8. Weitere Unterstützungspflichten

Die Auftragnehmerin unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

9. Meldung von Verletzungen des Schutzes personenbezogener Daten

Die Auftragnehmerin informiert den Auftraggeber über eine Verletzung des Schutzes personenbezogener Daten, die dessen Auftragsdaten betrifft, unverzüglich nach Kenntniserlangung, möglichst innerhalb von 24 Stunden und spätestens innerhalb von 48 Stunden. Die Mitteilung enthält die zu diesem Zeitpunkt verfügbaren Informationen zu Art, Umfang, betroffenen Daten- und Personenkategorien, voraussichtlichen Folgen und Maßnahmen. Noch nicht verfügbare Informationen werden unverzüglich nachgereicht.

10. Nachweis und Kontrolle

10.1 Die Auftragnehmerin weist die Einhaltung dieses Vertrags durch geeignete Dokumentation nach (u. a. Beschreibung der TOMs, Zertifikate/Testate der eingesetzten Rechenzentren, Auszüge aus dem Verzeichnis der Verarbeitungstätigkeiten).

10.2 Genügt das dem Auftraggeber im Einzelfall nachweislich nicht, kann er — höchstens einmal je Vertragsjahr, mit angemessener Ankündigung von mindestens 14 Tagen, zu üblichen Geschäftszeiten und ohne Störung des Betriebs — eine Überprüfung durchführen oder durch einen zur Verschwiegenheit verpflichteten Dritten durchführen lassen. Die Begrenzung auf eine Routineprüfung je Vertragsjahr und die angemessene Vorankündigung gelten nicht bei einem Datenschutzvorfall, einem begründeten Verdacht auf eine erhebliche Vertrags- oder Datenschutzverletzung oder einer Anordnung der zuständigen Aufsichtsbehörde.

11. Löschung und Rückgabe

Während der Vertragslaufzeit kann der Auftraggeber seine Daten jederzeit über die Exportfunktionen erhalten. Nach Vertragsende entscheidet der Auftraggeber, ob die Auftragsdaten zurückzugeben und anschließend zu löschen oder unmittelbar zu löschen sind. Soweit keine abweichende Weisung erfolgt, stehen die Daten noch 30 Tage in einem eingeschränkten Zugriff zum Export bereit. Nach Ablauf dieses Zeitraums löscht die Auftragnehmerin die Auftragsdaten unverzüglich, spätestens innerhalb von sieben Tagen, aus den produktiven Systemen.

Sicherungskopien werden bis zur turnusmäßigen Überschreibung gesperrt, nicht für andere Zwecke verarbeitet und innerhalb des technisch bestätigten Sicherungszyklus überschrieben (RDS-automatisierte Sicherungen: rollierendes 7-Tage-Fenster, technisch verifiziert 20.08.2026 anhand der acht vorhandenen Tages-Snapshots; zusätzlich ein manueller Dump vor jedem Deploy, die letzten 14 Dumps werden vorgehalten — deploy-, nicht kalendertagsbezogen, aktuell also kürzer als 14 Tage Abdeckung). Eine Wiederherstellung erfolgt nur zur Wiederherstellung des Gesamtsystems; anschließend wird die Löschung erneut durchgeführt. Gesetzliche Aufbewahrungspflichten der Auftragnehmerin bleiben unberührt.

12. Haftung

Es gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Nutzungsvertrags (AGB Ziff. 8).

13. Schlussbestimmungen

Es gilt deutsches Recht. Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag geht in datenschutzrechtlichen Fragen dieser Vertrag vor. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1 — Gegenstand der Verarbeitung

Zwecke: Dienstplanung, Arbeitszeiterfassung, Abwesenheitsverwaltung, Stunden- und Lohnvorbereitungs-Auswertungen, Team-Kommunikation zu Schichten, Datenimport aus Vorsystemen.

Kategorien betroffener Personen: Mitarbeitende und Aushilfen des Auftraggebers; Nutzer mit Verwaltungsrollen.

Datenkategorien: Stammdaten (Name, Kontaktdaten, Rolle, Standort/Arbeitsbereich); Vertragsdaten (Vertragstyp, Soll-/Wochenstunden, Urlaubsanspruch, Eintritt/Austritt); Bewegungsdaten (Schichten, Stempelzeiten, Pausen, Zuschlagszeiten, Stundenkonten); Abwesenheiten inkl. Art der Abwesenheit; vom Auftraggeber hochgeladene Dokumente; Protokolldaten (Audit-Log).

Zu den verarbeiteten Daten können besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO gehören, insbesondere gesundheitsbezogene Angaben zur Art einer Abwesenheit. Der Auftraggeber ist dafür verantwortlich, dass für die Erhebung und Verarbeitung dieser Daten eine einschlägige Rechtsgrundlage besteht und nur die für den jeweiligen Zweck erforderlichen Angaben verarbeitet werden. Die Auftragnehmerin verarbeitet diese Daten ausschließlich nach

dokumentierter Weisung und unter Anwendung der in Anlage 2 beschriebenen Schutzmaßnahmen. Horella speichert standardmäßig nur den Status „krankheitsbedingt abwesend"; Diagnosen und medizinische Freitexte werden produktseitig nicht erhoben.

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die Maßnahmen beschreiben den Ist-Zustand der Horella-Infrastruktur (Stand der letzten technischen Verifikation: 20.08.2026).

Hosting & physische Sicherheit: Betrieb ausschließlich bei Amazon Web Services, Region eu-west-1 (Irland); physische Zutritts- und Umgebungssicherheit durch AWS (Zertifizierungen u. a. ISO 27001, SOC 2 — Testate abrufbar).

Zugriffs- und Zugangskontrolle: Rollenbasiertes Berechtigungsmodell in der Software (Betrieb, Standorte, Verwaltungs-/Mitarbeiterrollen); logische Mandantentrennung auf Datenebene; administrative Systemzugriffe ausschließlich über AWS Systems Manager (keine offenen SSH-Zugänge), personalisiert und protokolliert; die administrativen Konsolen-Zugänge (drei Principals mit `AdministratorAccess`, Gruppe `LO_Admin`) sind mit Multi-Faktor-Authentifizierung geschützt (registriert, bestätigt 21.08.2026). Support-Zugriffe der Auftragnehmerin auf die Umgebung des Auftraggebers erfolgen ausschließlich über personalisierte, als Support gekennzeichnete Konten, sind für die Administratoren des Auftraggebers im Produkt sichtbar, enden automatisch nach spätestens 60 Minuten und werden einschließlich aller Aktionen im Prüfprotokoll des Auftraggebers festgehalten.

Übertragungskontrolle: Transportverschlüsselung (TLS) für sämtliche Verbindungen; E-Mail-Versand über Amazon SES aus eu-west-1.

Speicherkontrolle: Serverseitige Verschlüsselung ruhender Daten im Objektspeicher (S3 — technisch verifiziert 20.08.2026); Datei-Uploads in S3 mit zugriffsbeschränkten Bucket-Richtlinien. Die Verschlüsselung der Datenbank-Volumes ist als geplante Härtungsmaßnahme vorgesehen (Ziff. 5: Maßnahmen werden am Stand der Technik weiterentwickelt).

Eingabekontrolle: Append-only-Audit-Log — jede Änderung mit Vorher/Nachher-Wert, Akteur und Zeitstempel; abgeschlossene („locked") Zeiteinträge sind unveränderbar.

Verfügbarkeitskontrolle: Tägliche automatisierte Datenbanksicherungen (RDS, rollierendes 7-Tage-Fenster, technisch verifiziert 20.08.2026); zusätzlich ein manueller Sicherungsdump vor jedem Deploy (die letzten 14 Dumps); Monitoring mit externer Erreichbarkeitsprüfung und Alarmierung (zuletzt geprüft 18.08.2026); dokumentiertes Deploy-Verfahren; die Wiederherstellung aus Sicherungen ist als dokumentiertes Verfahren beschrieben.

Trennungsgebot: Getrennte Umgebungen für Entwicklung/Test und Produktion; Testdaten ohne echte Personaldaten.

Datenminimierung bei KI-Funktionen: Übermittlung an den KI-Dienst PII-minimiert (Strukturinformationen, interne Kennungen, Beispielzeilen statt vollständiger Datensätze); KI-Funktionen sind serverseitig deaktivierbar.

Organisation: Vertraulichkeitsverpflichtung aller Beteiligten; Prozess für Datenpannen (Ziff. 9); regelmäßige Überprüfung der Maßnahmen.

Anlage 3 — Unterauftragsverarbeiter

Unternehmen	Sitz	Leistung	Ort der Verarbeitung	Garantie bei Drittland
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg (R.C.S. B186284), handelnd durch ihre Niederlassung Deutschland, Anni-Albers-Str. 21, 80807 München (HRB 242240) — bestätigt anhand VAT Invoice EUINDE26-1588026 vom 01.08.2026	Luxemburg	Hosting (EC2), Datenbank (RDS/MySQL), Objektspeicher (S3), E-Mail-Versand (SES), DNS (Route 53), Zertifikate (ACM), Monitoring/Alarmierung (CloudWatch, SNS), administrativer Zugriff (SSM) — vollständige Dienste-Liste technisch verifiziert 20.08.2026	EU (eu-west-1, Irland) für Rechenzentrum/Datenbank/Speicher/E-Mail	—

Unternehmen	Sitz	Leistung	Ort der Verarbeitung	Garantie bei Drittland
Anthropic Ireland, Limited	Irland	KI-Funktionen: Spaltenzuordnung beim Import, Auslesen von Vertragsdaten aus hochgeladenen Verträgen, Planbefehle in natürlicher Sprache, Erklärtexte zu Ersatzvorschlägen sowie Antwortentwürfe für Support-Anfragen (intern, Antwort durch Menschen). Übermittelt werden beim Import die Spaltenüberschriften und die ersten drei Zeilen der Datei; beim Auslesen von Vertragsdaten das hochgeladene Vertragsdokument; bei Planbefehlen und Ersatzvorschlägen Vorname, interne Kennung sowie Schicht- und Stundenangaben; bei Support-Anfragen Betreff und Text der Anfrage ohne E-Mail-Adressen und Telefonnummern sowie Rolle und aufgerufene Seite.	USA	Standardvertragsklauseln (Modul 2/3) im Data Processing Addendum von Anthropic