Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO)

HRTime Personal-Analyst · Stand 17.11.2026

Präambel

Dieser Vertrag gilt zwischen dem Kunden eines kostenpflichtigen Pakets des HRTime Personal-Analyst (Verantwortlicher, im Folgenden „Kunde“) und der HRTime Software GmbH, Huyssenallee 13, 45128 Essen (Auftragsverarbeiter, im Folgenden „Anbieter“). Er konkretisiert die datenschutzrechtlichen Pflichten aus dem Nutzungsvertrag über das Paket (Hauptvertrag) und wird mit der Bestellung eines Pakets Bestandteil des Hauptvertrags (Art. 28 Abs. 9 DSGVO: elektronisches Format).

Für die Daten seines Benutzerkontos, die Abrechnung und die Kommunikation mit dem Kunden ist der Anbieter selbst Verantwortlicher; dafür gilt die Datenschutzerklärung, nicht dieser Vertrag.

§ 1 Gegenstand und Dauer

(1) Der Anbieter verarbeitet personenbezogene Daten, die der Kunde in der Anwendung speichert (Mitarbeiter und gespeicherte Auswertungen), ausschließlich in seinem Auftrag.

(2) Der Vertrag gilt, solange der Anbieter solche Daten für den Kunden speichert, also über die Laufzeit des Pakets hinaus bis zur Löschung nach § 9.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

(1) Zweck: Speichern, Anzeigen, Auswerten und Löschen von Personaldaten für die Berechnungen des Kunden (z. B. Urlaubsanspruch, Fristen, Entgeltfortzahlung, Kennzahlen). Die Verarbeitung erfolgt durch Speicherung in einer Datenbank und Berechnung auf dem Server.

(2) Art der Daten: Name, Vorname, optional Geburtsdatum und Abteilung der Mitarbeiter; gespeicherte Auswertungen mit Kurzbeschreibung, Ergebnis, Kennzahlen und den Eingaben der Berechnung. Je nach Rechner können Auswertungen Gesundheitsdaten (Arbeitsunfähigkeit, Schwangerschaft, Entbindung, Fehlgeburt, Schwerbehinderung) und damit besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) enthalten.

(3) Betroffene Personen: Beschäftigte, Bewerber und ehemalige Beschäftigte des Kunden.

§ 3 Weisungen

(1) Der Anbieter verarbeitet die Daten nur auf dokumentierte Weisung des Kunden (Art. 28 Abs. 3 lit. a DSGVO). Die Weisungen sind abschließend im Hauptvertrag, in diesem Vertrag und in der Bedienung der Anwendung durch den Kunden festgelegt (Anlegen, Ändern, Löschen). Weitere Weisungen erteilt der Kunde in Textform an info@hrtime.de.

(2) Ist der Anbieter der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, informiert er den Kunden unverzüglich und darf die Ausführung bis zur Bestätigung aussetzen.

(3) Ist der Anbieter durch Recht der Union oder eines Mitgliedstaats zu einer anderen Verarbeitung verpflichtet, teilt er dies dem Kunden vorher mit, sofern das Recht dies nicht verbietet.

§ 4 Vertraulichkeit

Personen, die beim Anbieter Zugang zu den Daten haben, sind auf die Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO). Zugriff auf Kundendaten erfolgt nur, soweit dies für Betrieb, Fehlerbehebung oder auf Weisung des Kunden nötig ist.

§ 5 Technische und organisatorische Maßnahmen

Der Anbieter trifft die in der Anlage beschriebenen Maßnahmen nach Art. 32 DSGVO. Er darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde genehmigt die folgenden Unterauftragsverarbeiter: Host Europe GmbH, Hansestraße 111, 51149 Köln – Bereitstellung des Servers (Rechenzentrum), auf dem Anwendung, Datenbank und

Datensicherung laufen (Ort der Verarbeitung: Deutschland).

(2) Weitere oder andere Unterauftragsverarbeiter setzt der Anbieter nur ein, nachdem er den Kunden mindestens vier Wochen vorher in Textform informiert hat. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund widersprechen; kommt keine Einigung zustande, kann er den Hauptvertrag außerordentlich kündigen und erhält den anteiligen Preis zurück.

(3) Der Anbieter verpflichtet Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten (Art. 28 Abs. 4 DSGVO). Eine Verarbeitung außerhalb der Europäischen Union findet nicht statt.

§ 7 Rechte der betroffenen Personen

Der Anbieter unterstützt den Kunden mit geeigneten Maßnahmen bei Anträgen betroffener Personen (Art. 12 bis 22 DSGVO, Art. 28 Abs. 3 lit. e DSGVO). Auskunft, Berichtigung und Löschung kann der Kunde in der Anwendung selbst vornehmen. Wendet sich eine betroffene Person an den Anbieter, leitet dieser die Anfrage unverzüglich an den Kunden weiter.

§ 8 Unterstützungspflichten, Datenschutzverletzungen

(1) Der Anbieter unterstützt den Kunden bei den Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung, Benachrichtigung, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der ihm vorliegenden Informationen (Art. 28 Abs. 3 lit. f DSGVO).

(2) Eine Verletzung des Schutzes personenbezogener Daten meldet der Anbieter dem Kunden unverzüglich, möglichst innerhalb von 24 Stunden nach Bekanntwerden, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt.

§ 9 Löschung und Rückgabe

(1) Der Kunde kann einzelne Mitarbeiter und Auswertungen jederzeit in der Anwendung löschen; das Löschen eines Mitarbeiters löscht auch seine Auswertungen. Mit der Löschung des Benutzerkontos unter „Mein Konto“ werden alle Mitarbeiter und Auswertungen des Kunden gelöscht.

(2) Nach dem Ende der Laufzeit bleiben die Daten zunächst gespeichert, damit der Kunde sie bei einer Verlängerung weiter nutzen kann. Auf Weisung des Kunden löscht der Anbieter sie vollständig (Art. 28 Abs. 3 lit. g DSGVO). Bis zum Ende der Laufzeit kann der Kunde seine Auswertungen über die Anwendung abrufen und ausdrucken; danach stellt der Anbieter sie ihm auf Anforderung vor der Löschung zur Verfügung (Rückgabe).

(3) Datensicherungen werden nach 14 Tagen überschrieben; gelöschte Daten sind danach auch dort entfernt.

§ 10 Nachweise und Kontrollen

Der Anbieter stellt dem Kunden die zum Nachweis der Pflichten aus Art. 28 DSGVO nötigen Informationen zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, durch den Kunden oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer (Art. 28 Abs. 3 lit. h DSGVO). Inspektionen sind mit angemessener Frist, in der Regel vier Wochen, anzukündigen und während der Geschäftszeiten ohne Störung des Betriebs durchzuführen.

§ 11 Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln des Hauptvertrags.

(2) Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag vor, soweit es um den Schutz personenbezogener Daten geht.

(3) Es gilt deutsches Recht. Änderungen und Ergänzungen bedürfen der Textform.

Anlage – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit – Zutritt: Der Server steht im Rechenzentrum des Unterauftragsverarbeiters in Deutschland mit dessen Zutrittskontrolle; der Anbieter hat keinen physischen Zugang.

Vertraulichkeit – Zugang: Verwaltung des Servers nur über verschlüsselte Verbindungen mit persönlichen

Zugangsdaten; Zugangsdaten der Anwendung liegen außerhalb des Webverzeichnisses.

Vertraulichkeit – Zugriff: Benutzerkonten mit bestätigter E-Mail-Adresse und Passwortregeln; Passwörter nur als Hash gespeichert; Sperre nach 5 Fehlversuchen für 15 Minuten; Begrenzung der Anfragen je IP-Adresse; Rollen Benutzer und Administrator.

Vertraulichkeit – Trennung: Jeder Datensatz gehört genau einem Benutzerkonto; die Anwendung liest und schreibt Mitarbeiter und Auswertungen ausschließlich gefiltert nach dem angemeldeten Konto.

Integrität – Übertragung: Alle Verbindungen ausschließlich über HTTPS (TLS); Schutz der Formulare gegen Cross-Site-Request-Forgery.

Integrität – Eingabe: Änderungen an Daten nur durch angemeldete Benutzer des jeweiligen Kontos; Zeitpunkt der Erstellung wird gespeichert.

Verfügbarkeit und Belastbarkeit: Tägliche Sicherung der Datenbank auf dem Server, Aufbewahrung 14 Tage; Überwachung des Zustands über eine Prüfadresse; Sicherheitsupdates des Betriebssystems und der Laufzeitumgebung.

Datensparsamkeit: Die kostenlosen Rechner speichern keine Eingaben; geteilte Links enthalten keine Entgelte und keine Krankheitsbezeichnungen.

Überprüfung: Die Maßnahmen werden bei Änderungen der Anwendung oder des Hostings und mindestens jährlich überprüft.

Ort, Datum, Unterschrift Kunde (Verantwortlicher)	HRTime Software GmbH (Auftragsverarbeiter)