Vereinbarung zur Auftragsverarbeitung für PAY8

Fassung vom 17. November 2026

1. Vertragsparteien und Geltung

Diese Vereinbarung gilt zwischen dem Unternehmen, das den PAY8-Nutzungsvertrag abschließt und diese Vereinbarung annimmt, als Verantwortlichem und der Haptoring GmbH als Auftragsverarbeiterin. Die Angaben des Verantwortlichen ergeben sich aus seinem Firmenkonto und dem dokumentierten Vertragsabschluss.

Haptoring GmbH, Widumer Tor 1, 44575 Castrop-Rauxel, Deutschland, Amtsgericht Dortmund HRB 17054, vertreten durch den Geschäftsführer Ehsan Erschadi. Kontakt für Weisungen, Datenschutzanfragen und Sicherheitsvorfälle ist info@pay8.de, telefonisch +49 2305 54 84 43. Das Kundenunternehmen benennt eine zuständige Kontaktperson und hält deren E-Mail-Adresse im Firmenkonto aktuell.

Die Vereinbarung ergänzt den PAY8-Nutzungsvertrag für die Verarbeitung personenbezogener Daten im Auftrag des Kundenunternehmens. Bei einer abweichenden Regelung im Nutzungsvertrag gehen die datenschutzrechtlichen Pflichten dieser Vereinbarung vor. Ein bestehendes Vertragsverhältnis wird durch einen technischen Umzug allein nicht umgestellt.

2. Gegenstand, Daten und betroffene Personen

PAY8 stellt einen browserbasierten Firmenbereich zur Verwaltung von Kunden, Angeboten, Rechnungen, Belegdateien und Zahlungsständen bereit. Haptoring verarbeitet die Daten zur Durchführung der vom Kundenunternehmen beauftragten Funktionen, zum erforderlichen Betrieb, zur Fehlerbehebung sowie zur Rückgabe und Löschung.

Die Verarbeitung umfasst Entgegennahme, Zuordnung zum Firmenkonto, Speicherung, Abfrage, Bearbeitung, Erstellung und Bereitstellung von Dokumenten, technisch erforderliche Übermittlung, Sicherung, Wiederherstellung, Export und Löschung.

Datenkategorien	Umfang
Kunden- und Geschäftsdaten	Namen, Firma, geschäftliche Anschrift, Kontaktangaben, Kundennummern und erforderliche Angaben zu Belegempfängern und Ansprechpartnern.
Beleg- und Zahlungsdaten	Leistungsbeschreibungen, Artikel, Mengen, Preise, Steuerangaben, Belegnummern und -daten, Beträge, Zahlungsstände sowie vom Kunden angegebene geschäftliche Bankverbindungen und Zahlungsangaben.
Dateien und Begleitangaben	Angebote, Rechnungen, sonstige zugehörige Geschäftsunterlagen, interne Notizen, Entwürfe, Originaldateien und Fassungsmetadaten.
Zugriffs- und Supportdaten	Rollen und Firmenzuordnung, erforderliche technische Zugriffsdaten, vorgangsbezogene Aktivitäten sowie Supportinhalte, soweit sie zur Bearbeitung im Auftrag benötigt werden.

Betroffen sind Kunden, Geschäftspartner und Belegempfänger des Kundenunternehmens, deren Ansprechpartner und Vertreter, berechtigte Beschäftigte und sonstige Personen, deren Daten der Verantwortliche für den Geschäftsvorgang bereitstellt. Freitexte und Dateien sollen auf erforderliche kaufmännische Angaben begrenzt bleiben. Für die reguläre Nutzung sind besondere Datenkategorien nach Art. 9 DSGVO und Daten nach Art. 10 DSGVO nicht vorgesehen. Ein gezielt darauf ausgerichteter Einsatz bedarf einer vorherigen Abstimmung zu Datenarten, Weisung und zusätzlichen Schutzmaßnahmen.

Geschäftsbelege werden als Dateien bereitgestellt und können auf ausdrückliche Aktion eines berechtigten Benutzers über den eigenen Maildienst an den gewählten Empfänger gesendet werden. Konto- und Passwortmails dienen der Kontoverwaltung. Bei Nutzung des optionalen KI-Assistenten werden die für den beauftragten Entwurf verwendeten Eingaben an die OpenAI-API übertragen. Diese können Namen, geschäftliche Kontaktdaten, Leistungen, Mengen und Preise enthalten. Die KI gibt einen bearbeitbaren deutschen Entwurf zurück. Der Benutzer entscheidet über Übernahme, Prüfung, Speicherung, Abschluss und Versand. Die interaktiven Beispiele auf der öffentlichen Website verwenden fiktive Daten. Externe Zahlungsabwicklung und Google-Anmeldung werden nur bei entsprechender gesonderter Freischaltung eingesetzt.

3. Weisungen und Verantwortung

Das Kundenunternehmen entscheidet über die Rechtsgrundlagen, Inhalte, Empfänger und Zwecke seiner Geschäftsdaten. Es informiert betroffene Personen und nimmt deren Rechte wahr. Berechtigte Eingaben und Aktionen im vereinbarten Funktionsumfang sind dokumentierte Weisungen. Weitere Weisungen werden über die genannte Kontaktstelle in Textform erteilt und nachvollziehbar festgehalten.

Haptoring verarbeitet Auftragsdaten ausschließlich entsprechend diesen Weisungen und dem vereinbarten Zweck. Gesetzlich verpflichtende Verarbeitungen teilt Haptoring dem Verantwortlichen vorab mit, soweit das Gesetz dies zulässt. Bei einer nach Einschätzung von Haptoring datenschutzwidrigen Weisung informiert Haptoring das Kundenunternehmen unverzüglich und setzt deren betroffenen Teil bis zur Klärung aus.

Für die eigene Vertragsverwaltung, eigene rechtliche Pflichten und eigene Sicherheitszwecke handelt Haptoring nach den entsprechenden Datenschutzhinweisen in eigener Verantwortlichkeit. Die Zuordnung eines Vorgangs richtet sich nach seinem konkreten Zweck.

4. Vertraulichkeit und Schutzmaßnahmen

Haptoring beschränkt Zugriffe auf die für die Leistung erforderlichen Personen und Zwecke. Befugte Personen sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht. Die Verpflichtung besteht nach Ende ihrer Tätigkeit fort.

Haptoring trifft unter Berücksichtigung des Risikos geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die für PAY8 geltenden Maßnahmen beschreibt Anlage 1. Technische Anpassungen dürfen das vereinbarte Schutzniveau nicht herabsetzen. Wesentliche Änderungen werden dokumentiert. Haptoring prüft die Wirksamkeit der Maßnahmen bei wesentlichen Änderungen und anhand der betroffenen Risiken.

5. Unterstützung und Sicherheitsvorfälle

Haptoring leitet Anfragen betroffener Personen zu Auftragsdaten unverzüglich an das Kundenunternehmen weiter und beantwortet sie nur auf dessen Weisung. Unter Berücksichtigung der Verarbeitung und der verfügbaren Informationen unterstützt Haptoring bei Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit sowie bei Datenschutz-Folgenabschätzungen und erforderlicher vorheriger Konsultation.

Eine bekannt gewordene Verletzung des Schutzes von Auftragsdaten meldet Haptoring dem Verantwortlichen unverzüglich. Die Meldung enthält die bereits verfügbaren Informationen zu Art und Umfang, betroffenen Daten und Personen, möglichen Folgen, ergriffenen oder vorgeschlagenen Maßnahmen sowie einer Anlaufstelle. Ergänzende Informationen werden ohne unangemessene Verzögerung nachgereicht. Haptoring dokumentiert den Vorfall und unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten.

6. Weitere Auftragsverarbeiter und Drittlandverarbeitung

Das Kundenunternehmen genehmigt den Einsatz der in Anlage 2 beschriebenen Unterauftragsverarbeiter allgemein. Haptoring informiert die benannte Kontaktperson mindestens 30 Kalendertage vor einer beabsichtigten Ergänzung oder Ersetzung. Das Kundenunternehmen kann vor dem vorgesehenen Einsatz aus datenschutzbezogenen Gründen widersprechen. Die Parteien klären den Einwand vor Beginn der betroffenen Verarbeitung.

Haptoring verpflichtet Unterauftragsverarbeiter vertraglich zu einem den Anforderungen dieser Vereinbarung entsprechenden Datenschutz und bleibt für deren Erfüllung verantwortlich. Informationen über deren Aufgaben und wesentliche Schutzmaßnahmen werden auf Anfrage bereitgestellt. Weitere Zugriffsmöglichkeiten durch Dienstleister

werden entsprechend ihrer tatsächlichen Rolle bewertet.

Soweit eine Verarbeitung außerhalb des EWR stattfindet, stellt Haptoring die hierfür erforderlichen Voraussetzungen nach Kapitel V DSGVO sicher. Dazu zählen eine zulässige Übermittlungsgrundlage und die je Datenfluss erforderlichen ergänzenden Maßnahmen. Verwendete Garantien und Informationen über ihre wesentlichen Inhalte können über die Datenschutzkontaktstelle angefordert werden.

7. Nachweise und Kontrollen

Haptoring stellt die zur Prüfung der Pflichten nach Art. 28 DSGVO erforderlichen Informationen bereit. Das Kundenunternehmen kann geeignete Nachweise prüfen und, soweit erforderlich, Kontrollen einschließlich Inspektionen selbst oder durch einen zur Vertraulichkeit verpflichteten unabhängigen Prüfer durchführen. Termin und Umfang werden unter Berücksichtigung des Prüfzwecks abgestimmt. Bei konkreten Vorfällen oder behördlichen Anforderungen ermöglichen die Parteien die erforderliche zeitnahe Prüfung.

Rechte anderer Kunden, Geschäftsgeheimnisse und Systemsicherheit sind zu schützen. Sie beschränken die gesetzlich erforderliche Nachweisführung nicht. Haptoring informiert das Kundenunternehmen über aufsichtsbehördliche Maßnahmen, soweit sie dessen Auftragsverarbeitung betreffen und eine Mitteilung zulässig ist.

8. Dauer, Rückgabe und Löschung

Die Vereinbarung gilt während der Auftragsverarbeitung und bis zur vollständigen Rückgabe oder Löschung. Das Kundenunternehmen kann vor der Beendigung die vorgesehenen Exporte und Belegdownloads nutzen und ergänzende Rückgabeanweisungen an die Kontaktstelle richten.

Nach Ende der Leistungen gibt Haptoring nach Wahl des Verantwortlichen die Auftragsdaten in einem verfügbaren strukturierten Export zusammen mit den zugehörigen Dateien zurück und löscht vorhandene Kopien oder löscht die Daten mit Bestätigung. Die Ausführung erfolgt unverzüglich nach Klärung und Prüfung der berechtigten Weisung. Gesetzliche Speicherungspflichten werden mit betroffenem Datenumfang, Grundlage und Dauer dokumentiert. Während einer solchen Speicherung bleibt der Zugriff auf den gesetzlichen Zweck beschränkt.

Manuelle Sicherungen sind auf den jeweiligen Wiederherstellungs- oder Prüfzweck beschränkt. Bei einer Löschanweisung werden auftragsbezogene Sicherungskopien in die Löschung einbezogen. Soweit eine sofortige selektive Bereinigung einer technischen Sicherung nicht möglich ist, werden die Daten für die weitere Verwendung gesperrt und mit dem Wegfall des Sicherungszwecks gelöscht. Eine Rücksicherung setzt die zwischenzeitlich erteilten Löschanweisungen erneut um.

Temporäre Ausgaben und zweckbezogene Supportkopien werden nach Erledigung ihres Vorgangs gelöscht, soweit kein dokumentierter zulässiger Aufbewahrungsgrund fortbesteht. Technische Protokolle dienen dem Betrieb und der Untersuchung von Fehlern und Sicherheitsereignissen. Speicherung und Zugriff werden auf diesen Zweck begrenzt.

9. Schlussbestimmungen

Die gesetzlichen Pflichten und Rechte der Parteien bleiben bestehen. Das Kundenunternehmen kann die Verarbeitung aussetzen lassen, wenn Haptoring diese Vereinbarung erheblich verletzt. Die gesetzlichen Möglichkeiten zur Beendigung bleiben erhalten. Nach einer Beendigung gelten die Rückgabe-, Lösch- und Vertraulichkeitsregeln fort.

Der Abschluss kann schriftlich oder elektronisch erfolgen. Die angenommene Fassung wird dem Vertragsverhältnis mit Datum und Abschlussnachweis zugeordnet. Ein erforderliches Update dieser Vereinbarung wird nachvollziehbar mitgeteilt und entsprechend den anwendbaren Vertragsregeln vereinbart.

Anlage 1 · Maßnahmen im PAY8-Startbetrieb

Schutzbereich	Konkrete Ausgestaltung
Mandanten- und Zugriffsschutz	Die App prüft Firmenzuordnung und Rolle serverseitig. Zugriffe auf geschützte Dateien werden an die Berechtigung gebunden. Die Produktions-App verwendet einen eigenen technischen Benutzer und private Datenpfade.
Anmeldung	Passwörter werden als Hash gespeichert. Sitzungs- und Formularschutz, Anfragelimits sowie E-Mail-Bestätigung schützen den Zugang. Die für das Konto angebotenen Sicherheitsfunktionen können zusätzlich genutzt werden.
Übertragung	HTTPS schützt die Browserverbindung und die Übermittlung an die KI-API. Cloudflare verarbeitet App-Anfragen als vorgeschalteter Dienst und baut eine eigene TLS-Verbindung zum Origin auf. Der eigene Plesk-/Postfix-Dienst nimmt E-Mails mit authentifiziertem STARTTLS entgegen. Die anschließende Zustellung folgt der Route des Empfängerpostfachs.
Datenintegrität	Belegdateien und maßgebliche Fassungen werden privat gespeichert. Dokument-Hashes binden entsprechende Datei- und Exportzugriffe. Änderungen an endgültigen Belegen erfolgen im vorgesehenen Korrekturablauf.
Betrieb und physischer Standort	Der Anwendungsserver steht bei STRATO in Deutschland. Die Verarbeitung im Cloudflare-Netz kann weitere Länder einbeziehen. Konfiguration und Zugänge werden auf den jeweiligen Betriebskontext beschränkt.
Sicherung und Wiederherstellung	Es bestehen Möglichkeiten für private Firmenexporte und manuelle betriebliche Sicherungen. Manuelle Sicherung und Wiederherstellung wurden geprüft. Im Startumfang ist kein bestimmtes automatisches Sicherungsintervall oder garantierter Wiederherstellungszeitpunkt vereinbart. Das Kundenunternehmen berücksichtigt eigene gesetzliche Aufbewahrungspflichten und bewahrt benötigte Exporte auf.
Protokolle	Die Apache-Accesslogs der App verwenden feste Platzhalter für Request, Referer und User-Agent. IP-Adresse, Zeitpunkt, Status und Bytezahl bleiben für die Betriebs- und Sicherheitskontrolle erhalten. Plesk rotiert nach einer Dateigröße von 10.240 KB. Die Dateigröße bestimmt keine feste Speicherdauer in Tagen. Zugriff und Aufbewahrung erfolgen zweckgebunden.
Support und Organisation	Berechtigte Supportzugriffe werden auf den erforderlichen Firmenkontext und Vorgang begrenzt. Vertraulichkeit, dokumentierte Weisungen, Prüfung von Sicherheitsmeldungen und die Vorfallbearbeitung richten sich nach dieser Vereinbarung.

Anlage 2 · Eingesetzte Unterauftragsverarbeiter

Anbieter	Tätigkeit und Datenfluss
STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland	Serverinfrastruktur für App-Daten, Belegdateien und die eigene Mailinstallation. Der für PAY8 verwendete Anwendungsserver steht in Deutschland. Verarbeitung und Aufbewahrung richten sich nach dem beauftragten Infrastrukturdienst und den dazugehörigen Anweisungen. STRATO AVV
Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA	Vermittlung und Schutz des Datenverkehrs zu app.pay8.de. Der Proxy verarbeitet IP-Adressen, Anfragedaten, HTTP-Header und die zur Bereitstellung und Absicherung erforderlichen Inhalte. Je Dienst können zusätzliche Sicherheits- und Protokolldaten sowie Cookies betroffen sein. Die Verarbeitung kann außerhalb des EWR erfolgen. Cloudflare DPA
OpenAI Ireland Ltd., Irland, einschließlich der für die API eingesetzten weiteren Auftragsverarbeiter	Erstellung von Text- und Belegentwürfen aus den auf Benutzeraktion übermittelten Angaben. Verarbeitung von Eingaben, Modellantworten und erforderlichen technischen Metadaten nach dem API-Vertrag und den dafür geltenden Datenkontrollen. Je Endpunkt und Einstellung können Inhalte auch für Sicherheitsprüfungen oder zur Bereitstellung der API gespeichert werden. Eine Verarbeitung außerhalb des EWR kann stattfinden. OpenAI DPA, API-Datenkontrollen

Die Kontaktstelle der Haptoring GmbH erteilt Auskunft zu den jeweils eingesetzten Dienstteilen und den zugehörigen Datenschutzgarantien. Bei einer Ortsabfrage ruft PAY8 die OpenPLZ-Schnittstelle serverseitig mit der eingegebenen deutschen Postleitzahl ab. Kundenname und Anschrift werden für diese Abfrage nicht übertragen. Die lokal eingesetzte Verwaltungs- und Mailsoftware Plesk/Postfix wird durch Haptoring auf der Serverinfrastruktur betrieben.

Diese Vereinbarung wurde anhand der Anforderungen von Art. 28 DSGVO und der Struktur des Durchführungsbeschlusses (EU) 2021/915 für PAY8 ausgearbeitet. DSGVO, Amtliche Standardvertragsklauseln