Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Verantwortlicher (Kunde)

_____
_____
_____

Auftragsverarbeiter

toFace Media, Handan Tas
Arnsberger Str. 22
51065 Köln

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO zwischen dem Kunden (Verantwortlicher, "Kunde") und toFace Media, Handan Tas, Arnsberger Str. 22, 51065 Köln (Auftragsverarbeiter, "toFace"). Stand: November 2026

§ 1 Gegenstand und Dauer

(1) toFace betreibt für den Kunden ein Online-Bestellsystem ("Hauptvertrag"). Dabei verarbeitet toFace personenbezogene Daten im Auftrag und nach Weisung des Kunden.

(2) Dieser AVV gilt, solange toFace Daten für den Kunden verarbeitet, längstens bis zur Löschung nach § 8. Er geht bei Widersprüchen zum Datenschutz den übrigen Regelungen des Hauptvertrags vor.

§ 2 Art, Zweck, Daten und Betroffene

Zweck: Bereitstellung und Betrieb des Bestellshops: Entgegennahme und Weiterleitung von Bestellungen, Kundenkonten, Zahlungsabwicklung über die Zahlungskonten des Kunden, Bestellbestätigungen und Status-Mails, Funktionen des gebuchten Pakets (z. B. Treuekarte, Gutscheine, Bewertungen, Telefonbestellung, Fahrer-Ansicht, Gäste zurückholen), Datensicherung, Wartung und Support.

Art der Verarbeitung: Erheben, Speichern, Ordnen, Abfragen, Anzeigen, Übermitteln an die vom Kunden gewählten Empfänger (z. B. Zahlungsanbieter, Bondrucker, Mitarbeiter), Sichern, Löschen.

Betroffene Personen: Gäste und Besteller des Kunden; Käufer und Empfänger von Geschenkgutscheinen; Anrufer bei Nutzung der Anruferkennung; Mitarbeiter, Fahrer und weitere Nutzer mit Zugang zum Admin-Bereich.

Datenarten:

- Kontaktdaten: Name, E-Mail-Adresse, Telefonnummer, Lieferanschrift (Straße, PLZ, Ort)
- Bestelldaten: bestellte Gerichte, Beträge, Bestellart, Wunschzeit, Anmerkungen, Tischnummer, Trinkgeld, eingelöste Rabatte und Gutscheine
- Zahlungsdaten: Zahlungsart, Zahlungsstatus, Transaktionsnummern der Zahlungsanbieter (keine vollständigen Karten- oder Kontodaten; diese verarbeitet allein der Zahlungsanbieter)
- Kundenkonto: Passwort (nur als Hash), Treuepunkte, persönliche Rabatte, Werbewiderspruch, Zeitpunkt der letzten Werbe-Mail, ggf. 2-Faktor-Daten
- Bewertungen (Sterne, Kommentar, Name) und Daten von Geschenkgutscheinen (Käufer, Empfänger, Nachricht)
- Anrufer-Telefonnummern (Anruferkennung)
- Zugangsdaten und Protokolle der Nutzer des Admin-Bereichs
- technische Daten: IP-Adressen und Zeitstempel in Server-Logfiles

Besondere Kategorien von Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. Gibt ein Gast freiwillig Gesundheitsangaben in eine Anmerkung ein (z. B. Allergien), werden diese nur zur Ausführung der Bestellung verarbeitet.

Ort der Verarbeitung: ausschließlich in Deutschland. Eine Verlagerung in ein Land außerhalb der EU bzw. des EWR bedarf der vorherigen Zustimmung des Kunden in Textform und der Voraussetzungen der Art. 44 ff. DSGVO.

§ 3 Weisungen

(1) toFace verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch bei Übermittlungen in Drittländer, es sei denn, toFace ist gesetzlich zur Verarbeitung verpflichtet; dann teilt toFace dies dem Kunden vorher mit, soweit das Gesetz es nicht verbietet. Der Hauptvertrag, dieser AVV und die Einstellungen, die der Kunde im Admin-Bereich vornimmt, sind die Weisungen.

(2) Weitere Weisungen erteilt der Kunde in Textform. toFace weist den Kunden unverzüglich darauf hin, wenn eine Weisung nach seiner Auffassung gegen Datenschutzvorschriften verstößt, und darf ihre Ausführung bis zur Bestätigung aussetzen.

§ 4 Pflichten von toFace

(1) toFace verpflichtet alle Personen, die Zugang zu den Daten haben, auf Vertraulichkeit, soweit sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) toFace trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO aus Anlage 1 und überprüft sie regelmäßig. toFace darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

(3) toFace unterstützt den Kunden bei seinen Pflichten aus Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen.

(4) toFace verwendet die Daten nicht für eigene Zwecke, insbesondere nicht für Werbung, und gibt sie nicht an Dritte weiter, außer an Unterauftragnehmer nach § 5. Ausgenommen sind zusammengefasste Bestellzahlen ohne Personenbezug (Anzahl und Umsatz je Zeitraum).

§ 5 Unterauftragnehmer

(1) Der Kunde stimmt dem Einsatz der in Anlage 2 genannten Unterauftragnehmer zu.

(2) toFace darf weitere Unterauftragnehmer einsetzen oder bestehende ersetzen (allgemeine Genehmigung). toFace informiert den Kunden mindestens vier Wochen vorher in Textform. Der Kunde kann der Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb von zwei Wochen widersprechen. Finden die Parteien keine Lösung, können beide den Hauptvertrag zum Zeitpunkt des Einsatzes außerordentlich kündigen.

(3) toFace verpflichtet jeden Unterauftragnehmer vertraglich auf dieselben Datenschutzpflichten wie in diesem AVV und haftet für ihn wie für eigenes Handeln.

(4) Keine Unterauftragsverarbeitung sind Nebenleistungen ohne Zugriff auf die Daten des Kunden (z. B. Telekommunikation, Domain-Registrierung). Zahlungsanbieter wie Stripe oder PayPal sind keine Unterauftragnehmer von toFace: Mit ihnen schließt der Kunde eigene Verträge, sie verarbeiten die Zahlungsdaten in eigener Verantwortung.

§ 6 Rechte der Betroffenen

(1) toFace unterstützt den Kunden mit geeigneten Maßnahmen dabei, Anträge von Betroffenen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu beantworten. Viele davon kann der Kunde selbst im Admin-Bereich erledigen.

(2) Wendet sich ein Betroffener direkt an toFace, leitet toFace die Anfrage unverzüglich an den Kunden weiter und beantwortet sie nicht selbst, außer auf Weisung des Kunden.

§ 7 Datenpannen

toFace meldet dem Kunden eine Verletzung des Schutzes der personenbezogenen Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, in Textform. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO und wird ergänzt, sobald weitere Informationen vorliegen. Die Meldung an Aufsichtsbehörde und Betroffene ist Sache des Kunden; toFace unterstützt dabei.

§ 8 Löschung und Rückgabe

(1) Nach Ende des Hauptvertrags gibt toFace dem Kunden auf Anforderung binnen 30 Tagen seine Daten in einem gängigen, maschinenlesbaren Format heraus. Danach löscht toFace die Daten einschließlich der Datenbank des Shops und bestätigt die Löschung auf Anfrage in Textform.

(2) Kopien in Datensicherungen werden im regulären Zyklus überschrieben, spätestens 14 Tage nach der Löschung. Bis dahin sind sie gegen Zugriff geschützt und werden nicht mehr verwendet.

(3) Daten, die toFace aufgrund gesetzlicher Pflichten länger aufbewahren muss, werden gesperrt und nach Ablauf der Frist gelöscht.

§ 9 Nachweise und Kontrollen

(1) toFace weist dem Kunden die Einhaltung dieses AVV auf Anfrage nach, insbesondere durch die Beschreibung der Maßnahmen in Anlage 1 und Nachweise der Unterauftragnehmer (z. B. Zertifizierungen des Rechenzentrums nach ISO/IEC 27001).

(2) Der Kunde kann sich nach Anmeldung mit angemessener Frist (in der Regel zwei Wochen) während der Geschäftszeiten selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer von der Einhaltung überzeugen, höchstens einmal im Jahr, außer bei konkretem Anlass. Den Aufwand von toFace trägt der Kunde, sofern keine Verstöße

festgestellt werden. Betriebs- und Geschäftsgeheimnisse sowie die Daten anderer Kunden bleiben geschützt.

§ 10 Haftung, Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO. Im Innenverhältnis gelten die Haftungsregeln des Hauptvertrags (§ 8 AGB), soweit Art. 82 DSGVO nicht entgegensteht.

(2) Änderungen dieses AVV bedürfen der Textform. Sollte eine Bestimmung unwirksam sein, bleibt der AVV im Übrigen wirksam. Es gelten deutsches Recht und der Gerichtsstand des Hauptvertrags.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- Zutritt: Server und Speicher stehen in Rechenzentren der Hetzner Online GmbH in Nürnberg (zertifiziert nach ISO/IEC 27001) mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal.
- Zugang zum Server: Anmeldung nur mit kryptografischem Schlüssel, Passwort-Anmeldung abgeschaltet; Firewall lässt nur die nötigen Dienste zu; Verwaltung nur durch toFace.
- Zugang zum Shop-Admin: persönliche Zugänge, Passwörter nur als Hash (bcrypt) gespeichert, 2-Faktor-Anmeldung verfügbar, Rollen (Mitarbeiter-Admin, Superadmin von toFace).
- Trennung: Jeder Kunde hat eine eigene Datenbank mit eigenem Datenbank-Benutzer und einen eigenen Speicherbereich für Bilder; Shops laufen in getrennten Containern.
- Datensparsamkeit: Karten- und Kontodaten der Gäste verarbeitet nur der Zahlungsanbieter; Entwürfe von Telefonbestellungen werden automatisch gelöscht; Testbestellungen werden beim Livegang gelöscht.

Integrität

- Alle Verbindungen zu Shop und Admin sind per TLS verschlüsselt (HTTPS); Zertifikate werden automatisch erneuert.
- Änderungen an Bestellungen und Einstellungen sind nur angemeldeten Nutzern mit passender Rolle möglich; Server-Logfiles dokumentieren Zugriffe.
- Werbe-Mails an Gäste enthalten einen Abmeldelink; Widersprüche werden im Kundenkonto gespeichert und beachtet.

Verfügbarkeit und Belastbarkeit

- Tägliche Datensicherung jeder Kunden-Datenbank; zusätzliche Kopie in einem getrennten Objektspeicher in Deutschland, Aufbewahrung 14 Tage.
- Monatlicher automatischer Wiederherstellungstest der Sicherungen mit Bericht.
- Überwachung der Erreichbarkeit jedes Shops im 5-Minuten-Takt mit Alarmierung.
- Automatische Sicherheitsupdates des Betriebssystems; Aktualisierung der Software ohne Unterbrechung des Betriebs.

Regelmäßige Überprüfung

- Überprüfung dieser Maßnahmen mindestens einmal jährlich und nach wesentlichen Änderungen.
- Verpflichtung aller Personen mit Datenzugang auf Vertraulichkeit; Zugriff nur, soweit für Betrieb und Support nötig.
- Dokumentierter Ablauf für Datenpannen (Erkennen, Eindämmen, Meldung an den Kunden nach § 7).

Anlage 2: Unterauftragnehmer

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen – Server, Datenbanken, Objektspeicher für Bilder und Datensicherungen – Deutschland (Nürnberg) – alle Daten nach § 2
- STRATO AG, Otto-Ostrowski-Straße 7, 10249 Berlin – Versand von E-Mails (Bestellbestätigung, Status, Gutscheine, Monatsbericht, Werbe-Mails mit Abmeldelink) – Deutschland – Name, E-Mail-Adresse, Inhalt der Mail
- komoot GmbH (Dienst "Photon"), Potsdam – Adressvorschläge und Entfernungsberechnung für Liefergebiete – Deutschland – eingegebene Lieferanschrift (Straße, PLZ, Ort), ohne Name

Leseexemplar. Abgeschlossen wird der AVV mit dem Vertrag, beim Online-Annehmen eines Angebots oder im Kundenbereich.