piid

Tasbasi Gruppe
Steekberg 5 · 24107 Kiel
+49 431 313030 · kontakt@mail.piid.me

Vertrag über die Auftragsverarbeitung (Art. 28 DSGVO)

Fassung 1.0 (27.10.2026)

zwischen [Name des Kunden], [Anschrift] – nachfolgend „Auftraggeber“ (Verantwortlicher) – und Tasbasi Gruppe, Steekberg 5, 24107 Kiel, vertreten durch Bülent Tasbasi – nachfolgend „Auftragnehmer“ (Auftragsverarbeiter) – zum Nutzungsvertrag Nr. [Vertragsnummer].

§ 1 Gegenstand und Dauer

Der Auftragnehmer stellt dem Auftraggeber die Software „piid“ bereit. Mit piid werden personenbezogene Daten von Reisenden aus den Systemen des Auftraggebers bereitgestellt und mithilfe einer Browser-Erweiterung in Formulare Dritter (z. B. Fluggesellschaften, Reedereien, Unterkünfte, Einreise- und Visumportale) übertragen. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien. Er gilt für die Laufzeit des Nutzungsvertrags und endet mit diesem, frühestens jedoch, wenn der Auftragnehmer keine personenbezogenen Daten des Auftraggebers mehr verarbeitet.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung umfasst – je nach Einstellung des Auftraggebers – das Entgegennehmen von Reisendendaten (per Schnittstelle, Tabellen-Upload oder Abruf aus einer vom Auftraggeber freigegebenen Tabelle), deren Speicherung, das Suchen und Bereitstellen für berechtigte Mitarbeitende des Auftraggebers sowie das Löschen.

Gewählte Datenhaltung: verschlüsselte Speicherung. Gespeicherte Datensätze werden nach 30 Tagen ohne Aktualisierung automatisch gelöscht. Der Auftraggeber kann Datenhaltung und Frist jederzeit im Kundenbereich ändern.

Zweck ist ausschließlich die Unterstützung des Auftraggebers beim Ausfüllen von Formularen für die Reisen seiner Kunden. Das Absenden von Formularen und damit die Übermittlung an Dritte erfolgt durch Mitarbeitende des Auftraggebers in eigener Verantwortung; der Auftragnehmer übermittelt keine Daten an die Betreiber der Formulare.

Beim Erfassen des Aufbaus eines Formulars (Scanner) werden keine personenbezogenen Daten verarbeitet, sondern nur Feldnamen, Beschriftungen und Auswahllisten.

§ 3 Art der Daten und Kreis der Betroffenen

Arten personenbezogener Daten:

- Identifikationsdaten: Name, Vorname, Geburtsname, Geschlecht/Anrede, Geburtsdatum und -ort, Staatsangehörigkeit
- Ausweis- und Reisedokumentdaten: Art, Nummer, Ausstellungsdatum und -ort, ausstellender Staat, Gültigkeit; Aufenthaltstitel
- Kontaktdaten: Anschrift, E-Mail, Telefon
- Angaben zur Familie: Vornamen der Eltern, Familienstand
- Reisedaten: Buchungsnummer, Reisedatum, Flugnummer, Unterkunft bzw. Gastgeber und Kontaktperson am Zielort
- Beruf
- Zugangs- und Protokolldaten der Mitarbeitenden des Auftraggebers (Name, E-Mail, Anmeldezeitpunkte, Abrufprotokoll)

Kreis der Betroffenen: Reisende und Kunden des Auftraggebers einschließlich mitreisender Personen und Minderjähriger; im Datensatz genannte Dritte (Eltern, Gastgeber, Kontaktpersonen); Mitarbeitende des

Auftraggebers.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. Der Auftraggeber stellt sicher, dass solche Daten nicht an piid übermittelt werden.

§ 4 Weisungen

Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Weisungen ergeben sich aus diesem Vertrag, dem Nutzungsvertrag und den Einstellungen, die der Auftraggeber in seinem Kundenbereich vornimmt (insbesondere Datenhaltung, Löschfristen, Benutzer und Berechtigungen). Weitere Weisungen erteilt der Auftraggeber in Textform.

Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin und darf die Ausführung bis zur Bestätigung aussetzen.

Eine Verarbeitung zu anderen Zwecken, insbesondere für eigene Zwecke des Auftragnehmers, ist ausgeschlossen, soweit der Auftragnehmer nicht gesetzlich dazu verpflichtet ist; in diesem Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vorab mit, sofern das Recht dies nicht verbietet.

§ 5 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit, soweit sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 1. Er darf sie weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er.

Die Verarbeitung findet ausschließlich in der Europäischen Union statt. Eine Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Textform und der Erfüllung der Art. 44 ff. DSGVO.

Der Auftragnehmer benennt dem Auftraggeber eine Ansprechperson für den Datenschutz: Bülent Tasbasi, kontakt@mail.piid.me.

§ 6 Unterauftragsverarbeiter

Der Auftraggeber stimmt der Beauftragung der in Anlage 2 genannten Unterauftragsverarbeiter zu.

Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen vorher in Textform über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen; kommt keine Einigung zustande, kann er den Nutzungsvertrag außerordentlich kündigen.

Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten.

§ 7 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12–22 DSGVO) sowie bei den Pflichten nach Art. 32–36 DSGVO. Anfragen betroffener Personen, die sich an den Auftragnehmer richten, leitet er unverzüglich an den Auftraggeber weiter.

Der Auftraggeber kann Daten jederzeit selbst über seinen Kundenbereich bzw. die Schnittstelle löschen.

§ 8 Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer informiert den Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden nach Bekanntwerden, über Verletzungen des Schutzes personenbezogener Daten des Auftraggebers. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO.

Der Auftragnehmer ergreift unverzüglich Maßnahmen zur Eindämmung und Aufklärung und stimmt diese mit dem Auftraggeber ab.

§ 9 Kontrollrechte

Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten auf Anfrage nach, insbesondere durch Auskünfte, Dokumentation der Maßnahmen gemäß Anlage 1 und Nachweise der Unterauftragsverarbeiter (z. B. Zertifizierungen).

Inspektionen vor Ort sind nach rechtzeitiger Anmeldung, in der Regel mit zwei Wochen Vorlauf, während der Geschäftszeiten und ohne Störung des Betriebs möglich. Kosten trägt jede Partei selbst, sofern nicht ein Verstoß des Auftragnehmers festgestellt wird.

§ 10 Löschung und Rückgabe

Gespeicherte Reisendendaten werden automatisch nach der vom Auftraggeber eingestellten Frist gelöscht; im Modus „nur durchreichen“ spätestens nach 24 Stunden bzw. – bei Abruf aus einer Tabelle des Auftraggebers – ohne Speicherung.

Nach Ende des Nutzungsvertrags löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers spätestens nach 30 Tagen, sofern keine gesetzliche Aufbewahrungspflicht besteht. Vor Ablauf dieser Frist kann der Auftraggeber eine Übergabe in einem gängigen Format (CSV oder JSON) verlangen. Vertrags-, Abrechnungs- und Protokolldaten, die gesetzlichen Aufbewahrungspflichten unterliegen, werden nach deren Ablauf gelöscht.

Datensicherungen werden im Rahmen der üblichen Rotationszyklen gelöscht.

§ 11 Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Information der betroffenen Personen und die Wahrung ihrer Rechte verantwortlich. Er übermittelt nur Daten, die er für die beschriebenen Zwecke verarbeiten darf.

Der Auftraggeber legt fest, welche Mitarbeitenden Zugang erhalten, hält Zugangsdaten und API-Schlüssel geheim und widerruft Zugänge ausgeschiedener Mitarbeitender unverzüglich.

Für die Übermittlung an Betreiber fremder Formulare – auch in Drittländer – ist allein der Auftraggeber verantwortlich.

Nutzt der Auftraggeber eine eigene Tabelle bei einem Drittanbieter (z. B. Google Tabellen) als Datenquelle, besteht das Vertragsverhältnis mit diesem Anbieter allein zwischen dem Auftraggeber und dem Anbieter.

§ 12 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO und den Haftungsregeln des Nutzungsvertrags.

§ 13 Schlussbestimmungen

Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Nutzungsvertrag vor.

Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, Kiel.

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

Vertraulichkeit

- Rechenzentren des Hosting-Dienstleisters in Deutschland mit Zutrittskontrolle, Videoüberwachung und Protokollierung (siehe Anlage 2)
- Zugang zur Anwendung nur mit persönlichem Konto; Passwörter ausschließlich als Hash (bcrypt) gespeichert; Sperre nach wiederholten Fehlversuchen
- Rollen und Berechtigungen: Mitarbeitende des Auftraggebers sehen nur die Daten ihres eigenen Mandanten
- Browser-Erweiterungen melden sich mit persönlichen, zeitlich begrenzten (90 Tage) und jederzeit widerrufbaren Zugängen an; gespeichert wird nur ein Hash

- Schnittstellen-Zugang nur mit API-Schlüssel; gespeichert wird nur ein Hash; Schlüssel einzeln sperrbar
- Gespeicherte Reisendendaten werden vollständig verschlüsselt (XChaCha20-Poly1305 bzw. AES-256-GCM). Der Schlüssel liegt getrennt von der Datenbank.
- Suche über nicht umkehrbare Kennungen (HMAC); in der Datenbank liegen keine Namen oder Passnummern im Klartext
- Trennung der Daten verschiedener Auftraggeber durch Mandantenkennung in jeder Abfrage

Integrität

- Übertragung ausschließlich verschlüsselt (TLS/HTTPS)
- Authentifizierte Verschlüsselung erkennt Veränderungen gespeicherter Daten
- Protokollierung von Anmeldungen, Abrufen von Reisendendaten und Änderungen an Zuordnungen, Benutzern und Schlüsseln
- Schutz gegen Fremdaufrufe (CSRF-Token, gesicherte Sitzungscookies), vorbereitete Datenbankabfragen gegen Einschleusung

Verfügbarkeit und Belastbarkeit

- Regelmäßige Datensicherungen durch den Hosting-Dienstleister
- Redundante Infrastruktur des Hosting-Dienstleisters, Schutz vor Überspannung und Brand
- Aktualisierung der eingesetzten Software

Datensparsamkeit und Löschung

- Wahl zwischen verschlüsselter Speicherung mit automatischer Löschfrist und „nur durchreichen“
- Automatisches Löschen abgelaufener Datensätze; manuelles Löschen jederzeit durch den Auftraggeber
- Hochgeladene Tabellen werden bis zum Import nur verschlüsselt und höchstens 30 Minuten zwischengespeichert
- Der Formular-Scanner überträgt keine eingegebenen Inhalte

Überprüfung

- Überprüfung der Maßnahmen bei wesentlichen Änderungen, mindestens jährlich
- Verpflichtung der Beschäftigten auf Vertraulichkeit

Anlage 2 – Unterauftragsverarbeiter

- IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland – Hosting von Anwendung und Datenbank, Rechenzentren in Deutschland

Zahlungsdienstleister, über die der Auftraggeber seine Rechnungen begleicht, verarbeiten keine Reisendendaten und sind keine Unterauftragsverarbeiter im Sinne dieses Vertrags.