

Smart Host

Vertrag zur Auftragsverarbeitung

Anhang I-IV

nach Art. 28 Abs. 6 DSGVO

(Standardvertragsklauseln der EU-Kommission)

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r):

Name	Anschrift	Name, Funktion und Kontaktdaten der Kontaktperson	Unterschrift und Beitrittsdatum

Auftragsverarbeiter:

Name	Anschrift	Name, Funktion und Kontaktdaten der Kontaktperson	Unterschrift und Beitrittsdatum
Smart Host GmbH	Am Kupfergraben 6 A, 10117 Berlin	Julian Leitner Geschäftsführer datenschutz@smart-h ost.com	

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden	• Hotelgäste • Interessenten für Hotelbuchungen • Bezieher von Hotel-Kommunikation
Kategorien personenbezogener Daten, die verarbeitet werden	Hotelgäste: • Stammdaten (Namen, Geburtsdatum) • Kontaktdaten (E-Mail-Adresse, Telefonnummer) • Adressdaten (Anschrift/en, Straße/n, PLZ, Ort) • Kommunikationspräferenzen • Buchungskanäle (z. B. Reiseveranstalter, Internet-Portal etc.), Buchungshistorie (soweit vorhanden), Gästebewertungen und sonstiges Feedback • Daten über die Inanspruchnahme der Leistungen des Hotelbetriebs, u.a. Übernachtungen, Zimmer, Datum, übernachtende Personen, gezahlte Preise, Gastronomie, Ratendetails, Zusatzwünsche wie Internet, Kategorie und Ausstattung des Zimmers, sonstige Kommentare etc.. • Präferenzen und Interessen • Daten über angefragte Hotelleistungen • Mitreisende • Daten zur Interaktion mit Hotel-Kommunikation (z.B. Öffnungsevents, Klickevents etc.) • Loyalitätsdaten (z.B. Statusniveau, Punkteanzahl) Interessenten: • Stammdaten (Name) • Kontaktdaten (E-Mail-Adresse, Telefonnummer) • Adressdaten (Anschrift/en, Straße/n, PLZ, Ort) • Kommunikationspräferenzen • Präferenzen und Interessen • Daten über angefragte Hotelleistungen, sonstige Kommentare • Daten zur Interaktion mit Hotel-Kommunikation (z.B. Öffnungsevents, Klickevents etc.) Bezieher von Hotel-Kommunikation: • wenn zutreffend: Stammdaten (Name) • Kontaktdaten (E-Mail-Adresse)

	• Kommunikationspräferenzen • Präferenzen und Interessen • Daten zur Interaktion mit Hotel-Kommunikation (z.B. Öffnungsevents, Klickevents etc.)
Art der Verarbeitung	Speicherung und Hosting von in der Verantwortung des Verantwortlichen liegenden personenbezogenen Daten im Zuge der Nutzung des Produkts des Auftragsverarbeiters durch den Verantwortlichen. Im Übrigen wird für die Beschreibung des Auftrags auf den zwischen den Parteien geschlossenen (Haupt-)Vertrag über die Nutzung des Dienstes/Produkts des Auftragsverarbeiters verwiesen.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden	Die Verarbeitung personenbezogener Daten erfolgt zur Unterstützung des Verantwortlichen bei der eigenverantwortlich festgelegten Nutzung der Gästeverwaltungsplattform des Auftragsverarbeiters. Die konkrete Festlegung der Verarbeitungszwecke obliegt dem Verantwortlichen. Der Auftragsverarbeiter verarbeitet die Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen, insbesondere zur: • Bereitstellung, Betrieb und technische Administration der Gästeverwaltungsplattform, • Entgegennahme, Speicherung, Organisation und Verwaltung von Gästedaten aus den vom Verantwortlichen genutzten Systemen, • Durchführung automatisierter, softwaregestützter Auswertungen im Auftrag des Verantwortlichen, • Bereitstellung der Verarbeitungsergebnisse zur Nutzung durch den Verantwortlichen im Rahmen des Dienstes. Die typischen, vom Verantwortlichen verfolgten Verarbeitungszwecke, die durch die Plattform unterstützt und vom Verantwortlichen beauftragt werden können, umfassen insbesondere: • Verwaltung und Pflege von Gästedaten, • Segmentierung von Gästen anhand definierter Kriterien (z. B. Aufenthaltsinformationen, Präferenzen), • Planung, Durchführung und Auswertung von Kommunikations- und

	Marketingmaßnahmen (z. B. Newsletter-Versand, Kampagnenmanagement), • Analyse des Gästeverhaltens und der Nutzung des Hotelangebots zur Verbesserung von Service und Ansprache, • Auswertung von Kampagnen- und Kommunikationsmaßnahmen (z. B. Öffnungsraten, Conversion, Interaktionen), • Erstellung aggregierter und individualisierter Reports zur Unterstützung betrieblicher Entscheidungen. • KI-Unterstützung zur Optimierung der Gästekommunikation (Erstellung von Textvorschlägen, Verbesserung und Optimierung bestehender Texte) sowie zur Zusammenfassung einzelner und Aggregation mehrerer Gästeprofile (z.B. Segment- oder Gruppenanalysen)
Dauer der Verarbeitung	Der Auftrag ist entsprechend der Laufzeit des (Haupt-)Vertrages erteilt und kann vom Verantwortlichen und/oder vom Auftragsverarbeiter entsprechend der Regelungen im (Haupt-)Vertrag gekündigt werden. Das Recht der Parteien zur fristlosen Kündigung bei Vorliegen der gesetzlichen Voraussetzungen bleibt hiervon unberührt.

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat Smart Host technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO getroffen, die nachfolgend aufgeführt werden.

A. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Smart Host ergreift Maßnahmen zur Gewährleistung der Vertraulichkeit. Hierunter fallen unter anderem Maßnahmen zur Zutritts-, Zugangs- und Zugriffskontrolle. Die in diesem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sollen eine angemessene Sicherheit gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Zutrittskontrolle/Gebäudeabsicherung

Unbefugten wird der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, durch folgende Maßnahmen verwehrt:

zu Büroräumen: Die Büroräume von Smart Host befinden sich in Berlin, Am Kupfergraben 6A – 10117 Berlin. In den Räumlichkeiten von Smart Host befindet sich keine kritische IT-Infrastruktur (Serversysteme). Dennoch wird der physikalische Zutritt zu Büroflächen größtmöglich durch Sicherheitsmaßnahmen geschützt:

- Das Gebäude und die Büroräume sind mit einem mechanischen Schließsystem versehen. Die Eingangsbereiche sind stets verschlossen. Die Schlüssel werden ausschließlich vom Management Team ausgegeben und bei den zugriffsberechtigten Personen selbst aufbewahrt. Die Schlüsselausgabe wird protokolliert.
- Betriebsfremde Personen müssen klingeln und sich persönlich anmelden. Sie werden beim Empfang angemeldet und dürfen sich nicht frei, sondern nur begleitet, in den Räumlichkeiten bewegen.
- Das Reinigungspersonal und weitere externe Dienstleister werden sorgfältig ausgewählt.

zu Serverräumen: Smart Host speichert personenbezogene Daten nicht auf eigenen Servern, sondern auf Grundlage einer Auftragsverarbeitung auf Servern des externen Dienstleisters Google (Google Cloud). Als Serverstandorte wurden die Google Rechenzentren Frankfurt, Deutschland (Zone europe-west3) sowie St. Ghislain, Belgien (Zone europe-west1) ausgewählt. Sämtliche Datenschutz- bzw. Sicherheitsmaßnahmen der Server werden von Google bereitgestellt und umgesetzt. Weitere Informationen finden sich unter <https://cloud.google.com/security> und <https://cloud.google.com/terms/data-processingaddendum#appendix-2-security-measures>.

Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Smart Host trägt dafür Sorge, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Zugriffe erfolgen auf Basis eines Berechtigungskonzepts. Es existiert ein definierter Freigabeprozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen. Benutzerrechte und Benutzerzugänge müssen bei der IT beantragt und genehmigt werden. Die Vergabe bzw. Änderungen von Zugriffsberechtigungen werden protokolliert.

- Smart Host gewährleistet, dass ausschließlich Personen Zugriff auf Daten erlangen, die diesen Zugriff zur Aufgabenerfüllung benötigen. Je nach Tätigkeitsgebiet des jeweiligen Mitarbeiters werden abgestufte Berechtigungen vergeben (rollenbasierter Zugriff je nach Abteilung). Hierbei wird stets nach dem Minimalprinzip gearbeitet. Die Anzahl der Systemadministratoren ist auf das Notwendigste reduziert.
- Das Speichern personenbezogener Daten auf mobilen Datenträgern ist untersagt. Alle personenbezogenen Daten werden ausschließlich in der Google Cloud abgelegt.

Zugangskontrolle/Absicherung Systemzugang

Durch folgende Maßnahmen wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Der Zugang zu personenbezogenen Daten ist nur für einen eingegrenzten Kreis an Mitarbeitern möglich. Die dienstlich bereitgestellten Arbeitsgeräte (Client-Rechner) werden nach den gängigen technischen Standards verschlüsselt und sind mit persönlichen Zugangsdaten (User-ID und Passwort) passwortgeschützt. Bei Verlust, Vergessen oder Ausspähen des Passworts setzt der Administrator ein neues Passwort, das der jeweilige Mitarbeiter nach der Erstanmeldung zu ändern hat.
- Eine Übersicht aller Client-Rechner wird unter Aufführung der jeweiligen Seriennummer stets aktuell geführt. Die Client-Rechner werden in den Büroräumen von Smart Host eingesetzt, können aber aufgrund von Geschäftsreisen oder zum Home Office auch außerhalb der Büroräume genutzt werden.
- Benutzerkennungen und Zugänge werden, wenn Mitarbeiter das Unternehmen verlassen, sofort gesperrt, bzw. gelöscht und somit die Zugangsrechte aufgehoben.
- Die Zugangskontrolle gewährleistet des Weiteren der Passwortschutz der Anwendungen und verschiedenen Dienste, die bei Smart Host eingesetzt und zur Verarbeitung personenbezogener Daten genutzt werden.

Fernzugang: Bei Fernzugängen erfolgt die Authentisierung ebenfalls mittels persönlicher Accounts inklusive Passwort-Eingabe. Je nach System ist ein VPN zwingend erforderlich.

Firewall: Die Systeme, auf denen die Daten verarbeitet werden, werden über eine Firewall abgesichert. Die Firewall wird regelmäßig aktualisiert.

Trennbarkeit

Smart Host trägt durch die nachfolgenden Maßnahmen dafür Sorge, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Die Speicherung erfolgt für jeden Mandanten/Kunden getrennt. Auftragsdaten (Gästedaten) und Vertragsdaten des Auftraggebers (Name, Anschrift) werden ebenfalls voneinander getrennt gespeichert. Die Trennung der Daten wird so gestaltet, dass eine Vermischung von Daten für unterschiedliche Verarbeitungszwecke nicht möglich ist. Bei der Datenerfassung wird eine Herkunft hinterlegt. Über Filter in der Software wird sichergestellt, dass nur Daten bearbeitet werden können, die zu einem bestimmten Zweck erhoben wurden. Produktiv- und Testsystem werden strikt getrennt.

B. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Smart Host ergreift Maßnahmen zur Gewährleistung der Integrität. Hierunter fallen unter anderem Maßnahmen zur Kontrolle der Weitergabe und Eingabe von Daten.

Transport- und Übertragungskontrolle (Sicherheit beim Datentransfer)

Smart Host trägt dafür Sorge, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird und dass

überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Datenübermittlung an Dienstleister und andere berechtigte Datenempfänger findet ausschließlich digital und verschlüsselt statt und wird systemseitig dokumentiert. Der Transfer personenbezogener Daten erfolgt durchweg verschlüsselt über E-Mail, verschlüsselter Datei als Mailanhang, per PGP/S/MIME, VPN, per SFTP sowie mit https/TLS. Auf Kundensysteme wird über verschlüsselte Verbindungen zugegriffen. Die Schlüssel bzw. Zertifikate verwaltet die eigene IT von Smart Host.

Eingabekontrolle

Smart Host gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Alle Eingaben werden vom Auftraggeber selbst vorgenommen oder in Auftrag gegeben.

C. Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Smart Host ergreift Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit.

Verfügbarkeitskontrolle

Smart Host trägt dafür Sorge, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Smart Host betreibt keine eigenen Serverressourcen in eigenen Rechenzentren, sondern greift auf die unter A. aufgeführten Google-Rechenzentren zurück, um eine bestmögliche Verfügbarkeit der eingesetzten Systeme zu gewährleisten. Der unterbrechungsfreie Betrieb der Server wird u.a. durch folgende Maßnahmen gewährleistet:

- Monitoring/Überwachung der Systemaktivitäten durch unsere Mitarbeiter
- Sicherung der Produktivumgebung in regelmäßigen Abständen/Datenspiegelung
- Absicherung der Systeme durch eine unterbrechungsfreie Stromversorgung (USV)
- Einsatz einer mehrschichtigen Virenschutz- und Firewall-Architektur
- Feuer-, Wasser- und Temperaturfrühwarnsysteme sowie Brandschutztüren, Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in den Serverräumen
- getrennte Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden
- regelmäßiges Patch-Management
- regelmäßiges Durchführen von Penetrations- und Belastungstests
- regelmäßige Trainings des eingesetzten Personals
- Datensicherung auf Basis eines Backup- und Recovery-Konzepts

Weitere Informationen finden sich unter:
<https://cloud.google.com/terms/data-processing-addendum#appendix-2security-measures>

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Smart Host gewährleistet, dass eingesetzte Systeme im Störfall wieder hergestellt werden können.

Auf der Basis eines Backup- und Recovery-Konzepts ist eine kurzfristige Wiederherstellung sichergestellt. Die Wirksamkeit des Konzepts wird durch regelmäßige Kontrollen überprüft.

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

Gemäß Art. 32 Abs. 1 lit. d DSGVO hat Smart Host ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etabliert. Prozesse und Systeme werden regelmäßig auf Datensicherheit und Qualität überprüft.

Auftragskontrolle

Gemäß Art. 32 Abs. 1 lit. d DSGVO, Art. 28 Abs. 1 DSGVO gewährleistet Smart Host, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Auswahl eingesetzter (Unter-)Auftragsverarbeiter erfolgt unter Sorgfaltsgesichtspunkten, insbesondere hinsichtlich der Datensicherheit. Dort wo erforderlich, werden mit (Unter-)Auftragsverarbeitern, die für Smart Host personenbezogene Daten im Auftrag verarbeiten, schriftliche Verträge zur Auftragsverarbeitung nach Maßgabe von Art. 28 Abs. 3 DSGVO abgeschlossen. Smart Host erteilt den (Unter-)Auftragsverarbeitern Weisungen und übt seine Kontrollrechte stichprobenartig aus. Es wird eine Liste der eingesetzten (Unter-)Auftragsverarbeiter geführt. Diese Liste stellt Smart Host auf Anfrage zur Verfügung.

Incident-Response-Management

Bei Smart Host existiert ein Team, das sich um etwaige Datenschutzvorfälle kümmert. Die Teammitglieder werden regelmäßig zum Umgang mit Datenschutzvorfällen geschult.

Datenschutzmanagement

Smart Host gewährleistet einen Prozess zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen, u.a. durch folgende Maßnahmen:

- Smart Host hat schriftlich einen Datenschutzbeauftragten bestellt. Dieser steht den Mitarbeitern wie Externen in Datenschutzfragen zur Verfügung und wird bei ggf. notwendigen Datenschutzfolgenabschätzungen und Datenschutzvorfällen eingebunden.
- Smart Host führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
- Verfahren, Verzeichnisse, Verträge, etwaige Datenschutzvorfälle und Behördenanfragen werden zu Dokumentations- und Transparenzzwecken in einem internen Datenschutzmanagementsystem vorgehalten.
- Alle Mitarbeiter werden auf die Vertraulichkeit verpflichtet und mit den Themen Datenschutz und Datensicherheit vertraut gemacht.
- Smart Host überprüft regelmäßig, ob/in welchem Umfang Zugangsrechte noch erforderlich sind.
- Wenn es aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewandt.
- Es existiert eine definierte Vertreterregelung innerhalb von Funktionsgruppen.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme der auf www.smart-host.com/trust abrufbaren Unterauftragsverarbeiter genehmigt.