Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO

Version	4.0
Stand	17.11.2026
Bearbeiter	Sonja Anschütz
Ersetzt	alle früheren Fassungen (zuletzt Version 3.3 vom 20.10.2026)

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch die SoftTec GmbH (Auftragnehmer) im Auftrag des Kunden (Auftraggeber) nach Art. 28 DSGVO. Der Auftragnehmer verarbeitet die Daten nur nach dokumentierter Weisung des Auftraggebers und schützt sie durch geeignete technische und organisatorische Maßnahmen.

Die Vertragsparteien schließen folgenden Vertrag:

AUFTRAGGEBER
Verantwortlicher

Firma

Straße, Hausnummer

PLZ, Ort, Land

Kundennummer

Weisungsberechtigte Person(en) (§ 3.2)

Ansprechpartner Datenschutz

AUFTRAGNEHMER
Auftragsverarbeiter

SoftTec GmbH
Firma

Hindelanger Straße 35
Straße, Hausnummer

87527 Sonthofen, Deutschland
PLZ, Ort, Land

Oliver Anschütz
Geschäftsführer

Amtsgericht Kempten, HRB 4662
Handelsregister

Olga Stepanova (Datenschutzbeauftragte), datenschutz@softtec.de
Ansprechpartner Datenschutz

§ 1 Gegenstand

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers nach Art. 28 DSGVO. Gegenstand, Art und Zweck der Verarbeitung, Datenarten und betroffene Personen stehen in Anlage 1. Es gelten die Teile der Anlagen 1 und 3, die zu den im Hauptvertrag gebuchten Produkten gehören.

1.2 Der Auftragnehmer verarbeitet die Daten grundsätzlich in der EU bzw. im EWR. Übermittlungen in ein Drittland erfolgen nur unter den Voraussetzungen der Art. 44 ff. DSGVO; Anlage 3 gilt insoweit als dokumentierte Weisung des Auftraggebers.

§ 2 Vertragslaufzeit

Dieser Vertrag gilt für die Laufzeit des Hauptvertrags und darüber hinaus, solange der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet. Der Auftragnehmer kann ihn ändern, soweit dies rechtlich erforderlich ist oder das Schutzniveau nicht sinkt. Er zeigt die Änderung mindestens sechs Wochen vor Wirksamwerden in der Software an; widerspricht der Auftraggeber nicht binnen zwei Wochen nach Zugang, gilt sie als angenommen, worauf die Anzeige hinweist. Widerspricht der Auftraggeber, gilt die bisherige Fassung fort; jede Partei kann den Hauptvertrag dann mit einer Frist von vier Wochen kündigen. Eine neue Fassung ersetzt die bisherige vollständig. Für Änderungen der Anlagen 2 und 3 gelten §§ 6 und 7.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

3.1 Der Auftraggeber ist Verantwortlicher; er beurteilt die Zulässigkeit der Verarbeitung und wahrt die Rechte der betroffenen Personen. Wendet sich eine betroffene Person an den Auftragnehmer, verweist er sie an den Auftraggeber; bei der Beantwortung unterstützt er diesen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

3.2 Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, außer er ist nach dem Recht der EU oder eines Mitgliedstaats dazu verpflichtet; dann informiert er ihn vorab, soweit das Recht dies nicht verbietet. Weisungsberechtigt sind die im Vertragskopf genannten Personen; Änderungen teilt der Auftraggeber unverzüglich in Textform mit.

3.3 Die technische und organisatorische Umsetzung legt der Auftragnehmer im Rahmen von § 6 fest.

3.4 Weisungen erfolgen in Textform. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich und darf sie bis zur Bestätigung oder Änderung aussetzen. Weisungen über den vereinbarten Leistungsumfang hinaus sind Änderungswünsche und werden gesondert vergütet.

§ 4 Kontrollbefugnisse des Auftraggebers

4.1 Der Auftragnehmer weist die Einhaltung seiner Pflichten vorrangig durch aktuelle Zertifikate, Prüfberichte oder Selbstauskünfte nach, etwa nach ISO/IEC 27001. Darüber hinaus ermöglicht er Überprüfungen einschließlich Vor-Ort-Kontrollen durch den Auftraggeber oder einen von ihm beauftragten Prüfer und wirkt daran mit; Vor-Ort-Kontrollen sind höchstens einmal je Kalenderjahr zulässig, außer bei begründetem Verdacht auf einen Verstoß gegen diesen Vertrag.

4.2 Eine weisungsberechtigte Person (§ 3.2) kündigt die Kontrolle mindestens vier Wochen vorher in Textform an und benennt den Prüfer; bei begründetem Verdacht genügt eine kürzere angemessene Frist. Prüfer müssen zur Vertraulichkeit verpflichtet sein und dürfen nicht im Wettbewerb mit dem Auftragnehmer stehen, sonst kann er sie ablehnen. Kontrollen finden zu den üblichen Geschäftszeiten und ohne vermeidbare Betriebsstörung statt; Daten anderer Kunden werden nicht offengelegt.

4.3 Die Kosten einer Kontrolle trägt der Auftraggeber; den Aufwand des Auftragnehmers vergütet er nach dem Hauptvertrag.

§ 5 Pflichten des Auftragnehmers

5.1 Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes von dessen personenbezogenen Daten unverzüglich, nachdem sie ihm mit hinreichender Sicherheit bekannt geworden sind, und unterstützt ihn bei dessen Pflichten nach Art. 32 bis 36 DSGVO. Unterstützungsleistungen nach § 3.1 und diesem Absatz, die nicht auf einem Verstoß des Auftragnehmers beruhen, vergütet der Auftraggeber nach dem Hauptvertrag.

5.2 Der Auftraggeber kann vor Vertragsende selbst kostenfrei eine vollständige Kopie sämtlicher Anwendungsdaten exportieren. Verlangt er binnen 30 Tagen nach Vertragsende in Textform eine Kopie, übersendet ihm der Auftragnehmer diese gegen gesonderte Vergütung auf üblichen Datenträgern. Danach löscht der Auftragnehmer die personenbezogenen Daten, soweit keine gesetzliche Pflicht zur Speicherung besteht. Datensicherungen werden im Rahmen der regulären Sicherungsrotation gelöscht (Anlage 2).

§ 6 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die Maßnahmen nach Art. 32 DSGVO; die aktuellen Maßnahmen stehen in Anlage 2. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt; auf Anfrage erhält der Auftraggeber die aktuelle Fassung der Anlage 2.

§ 7 Einsatz von Unterauftragsverarbeitern (Subunternehmern)

7.1 Der Auftraggeber genehmigt allgemein den Einsatz von Subunternehmern; die in Anlage 3 genannten gelten als genehmigt.

7.2 Will der Auftragnehmer einen Subunternehmer hinzufügen oder ersetzen, informiert er die betroffenen Auftraggeber vorab per E-Mail oder durch Hinweis in der Software. Der Auftraggeber kann binnen zwei Wochen nach Zugang aus einem anzugebenden wichtigen datenschutzrechtlichen Grund widersprechen; sonst gilt die Änderung als genehmigt. Vor Fristablauf setzt der Auftragnehmer den Subunternehmer nur ein, wenn es für Betrieb oder Sicherheit sofort erforderlich ist. Nach einem Widerspruch setzt er ihn für den Auftraggeber nicht ein, soweit dies möglich ist; andernfalls kann jede Vertragspartei die Nutzung des betroffenen Produkts oder Moduls innerhalb von vier Wochen nach dem Widerspruch beenden. Betrifft der Subunternehmer die Grundfunktion der Plattform, gilt dies für den Hauptvertrag.

7.3 Der Auftragnehmer verpflichtet Subunternehmer vertraglich auf ein gleichwertiges Datenschutzniveau. Bei Anbietern mit Standardverträgen genügen deren Auftragsverarbeitungsbedingungen; Kontrollen erfolgen dort über deren Zertifikate und Prüfberichte.

7.4 Dienstleister für reine Nebenleistungen, etwa Telekommunikation, Post- oder Reinigungsdienste, sind keine Subunternehmer im Sinne dieses Vertrags. Drittsysteme, die der Auftraggeber selbst beauftragt und über Schnittstellen anbindet (z. B. Channel-Partner, Buchhaltungssoftware), sind keine Subunternehmer; die Übermittlung dorthin erfolgt auf Weisung des Auftraggebers.

§ 8 Geheimhaltungspflicht

Der Auftragnehmer gewährt Personen erst Zugang zu den Daten, nachdem sie zur Vertraulichkeit verpflichtet wurden. Im Übrigen gilt die Geheimhaltungsregelung des Hauptvertrags.

§ 9 Schlussbestimmungen

Für Abschluss und Änderungen dieses Vertrags genügt die Textform oder die Bestätigung in der Software; §§ 2, 6 und 7 bleiben unberührt. Die Anlagen sind Bestandteil dieses Vertrags; bei Widersprüchen geht er dem Hauptvertrag vor.

Für den Auftraggeber

_____
Ort, Datum

_____
Unterschrift

Für den Auftragnehmer

Sonthofen, den _____



_____
Unterschrift

Anlage 1

Auftragsdetails nach Produkten

Dieser Vertrag umfasst die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der vertraglich vereinbarten Leistungen aus dem Hauptvertrag.

Teil A · Für alle Produkte	Gilt für jeden Auftraggeber: Leistungen, Datenarten, betroffene Personen und Subunternehmer, die produktübergreifend gelten. Welche davon anfallen, hängt vom gebuchten Produkt ab. Für die hotline Hotelsoftware (lokal installiert) und Easy2Bon mit lokaler TSE gilt nur Teil A.
Teil B · Je gebuchtem Produkt	Gilt nur für die Produkte, die der Auftraggeber im Hauptvertrag gebucht hat: SoftTec Cloud Hotelsoftware · SoftTec Payment · RESERVATE · SoftTec Chatbot · hotlineCloud · Caesar Data · Easy2Bon mit Cloud-TSE

Teil A: Für alle Produkte

Leistungen	Wartung, Support und Fernwartung (TeamViewer)
Zugriff auf die Daten	Welche Systeme der Auftragnehmer betreut, ergibt sich aus dem Hauptvertrag. Fernwartung erfolgt über TeamViewer; der Auftraggeber kann die Arbeiten am Bildschirm mitverfolgen. Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o. ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.
Datensicherung	Bei lokal installierter Software (hotline Hotelsoftware, Easy2Bon) liegt die Datensicherung in der Verantwortung des Auftraggebers. Ist für die hotline Hotelsoftware die Datensicherung gebucht, übernimmt sie der Auftragnehmer über comtrance (Anlage 3, Nr. 9). Für die Produkte nach Teil B siehe dort.
Datenarten	Stammdaten: Personenstammdaten · Kommunikationsdaten · Benutzerdaten der Mitarbeitenden des Auftraggebers Buchung und Aufenthalt: Vertrags- und Buchungsdaten · Meldedaten nach § 30 BMG Abrechnung: Abrechnungs- und Zahlungsdaten Sonstige: Protokolldaten · Sonstige vom Auftraggeber in der Software erfasste Daten *Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) verarbeitet der Auftragnehmer nur, soweit der Auftraggeber sie in der Software erfasst, etwa Allergie- oder Gesundheitsangaben in Freitextfeldern. Für die Zulässigkeit dieser Erfassung ist allein der Auftraggeber verantwortlich.*
Betroffene Personen	Kunden des Auftraggebers: natürliche Personen, die Leistungen oder Produkte des Auftraggebers in Anspruch nehmen, einschließlich Ansprechpartnern von Firmenkunden Interessenten: Personen, die beim Auftraggeber anfragen, etwa ein Angebot, ohne zu buchen Mitreisende und Begleitpersonen: Personen ohne eigene vertragliche Beziehung zum Auftraggeber, deren Daten z. B. beim Check-in über den Kiosk, die Gäste-App oder den digitalen Meldeschein erfasst werden Mitarbeitende des Auftraggebers: Beschäftigte, die im Rahmen der vertraglichen Leistungen mit dem Auftragnehmer in Kontakt stehen oder dessen Software nutzen
Ort und Subunternehmer	Es gilt § 1.2. Für alle Produkte setzt der Auftragnehmer die in Anlage 3 unter „Für alle Produkte“ genannten Subunternehmer ein (Nr. 1 bis 5). Für die hotline

	Hotelsoftware kommt Nr. 9 (comtrance) hinzu.

Teil B: Je Produkt

SoftTec Cloud Hotelsoftware

Leistungen	Betrieb der Hotelsoftware als Cloud-Dienst, einschließlich Gäste-Account, digitalem Meldeschein, Ressourcenverwaltung, Modul KassenSichV und E-Mail-Versand über Brevo, SMS-Versand über chatlyn · Add-ons, soweit gebucht: Buchungsmaschine (IBE), Channelmanager, Angebotsmanager, Check-in-Kiosk, Digitale Türöffnung
Zugriff auf die Daten	Mitarbeiter des Auftragnehmers greifen für Support und Einrichtung über ihre personenbezogenen SoftTec-Konten direkt auf das Profil des Auftraggebers zu. Die Fernwartungssoftware TeamViewer wird nur im Bedarfsfall eingesetzt, etwa um Abläufe gemeinsam mit dem Auftraggeber am Bildschirm zu zeigen.
Datensicherung	Durch den Auftragnehmer, siehe Anlage 2, „Kontrolliertes Backup- und Recoverykonzept“.
Subunternehmer	Anlage 3, Nr. 6, 7, 8 und 8a (HERE, Microsoft, Brevo, chatlyn); für das Modul KassenSichV zusätzlich Nr. 10 und 11 (Ruthardt, TERRA CLOUD). efsta (Nr. 15) handelt als eigener Verantwortlicher.

SoftTec Payment

Leistungen	Zahlungsabwicklung für die SoftTec Cloud Hotelsoftware und RESERVATE. Der Auftragnehmer erhält dabei nur Token, keine vollständigen Kartendaten.
Datensicherung	Durch den Auftragnehmer, siehe Anlage 2, „Kontrolliertes Backup- und Recoverykonzept“.
Subunternehmer	Keine. Adyen (Nr. 13) und Datatrans (Nr. 14) handeln als eigene Verantwortliche.

RESERVATE

Leistungen	Betrieb der Plattform RESERVATE, eigenständig oder als Add-on zur SoftTec Cloud Hotelsoftware
Besondere Kategorien	Angaben zu Allergien, soweit sie bei der Reservierung erfasst werden (Art. 9 DSGVO)
Datensicherung	Durch den Auftragnehmer, siehe Anlage 2, „Kontrolliertes Backup- und Recoverykonzept“.
Subunternehmer	Anlage 3, Nr. 2 (IONOS, Hosting) und Nr. 12 (Google, reCAPTCHA); für die Zahlungsabwicklung siehe SoftTec Payment

SoftTec Chatbot

Leistungen	Betrieb des SoftTec Chatbots in einem eigenen Konto je Auftraggeber. Der Auftragnehmer wertet Fragen aus, die der Chatbot nicht beantworten konnte,

	und ergänzt die Antworten für den jeweiligen Auftraggeber. Gesprächsinhalte werden weder für andere Auftraggeber noch zum Training von KI-Modellen verwendet.
Datensicherung	Durch Chatbase. Die Produktivdatenbanken werden täglich, wöchentlich und monatlich gesichert; die Wiederherstellung wird regelmäßig getestet. Die Backups sind verschlüsselt (AES-256), die Übertragung erfolgt per TLS 1.2. Nach Vertragsende oder auf Löschanfrage werden die Daten einschließlich der Backups innerhalb von 30 Tagen gelöscht. Chatbase ist nach SOC 2 Type II geprüft.
Subunternehmer	Anlage 3, Nr. 16 (Chatbase)

hotlineCloud

Leistungen	Hosting, Betreuung und Datensicherung der hotline Hotelsoftware auf einem eigenen Server je Auftraggeber
Datensicherung	Durch den Auftragnehmer, siehe Anlage 2, „Kontrolliertes Backup- und Recoverykonzept“.
Subunternehmer	Anlage 3, Nr. 10 und 11 (Ruthardt, TERRA CLOUD)

Caesar Data

Leistungen	Betrieb der Online-Buchungsstrecke (Direktbuchung über die Website des Auftraggebers) und der Hotelverwaltung (Verfügbarkeiten, Preise, Reservierungen) einschließlich Versand von Reservierungsbestätigungen an Gäste
Datensicherung	Durch den Auftragnehmer im Rechenzentrum von comtrance (Anlage 3, Nr. 9).
Subunternehmer	Anlage 3, Nr. 9 (comtrance, Hosting und Mailversand). Online-Zahlungen über Datatrans (Anlage 3, Nr. 14), das als eigener Verantwortlicher handelt.

Easy2Bon mit Cloud-TSE

Leistungen	Cloud-TSE für Easy2Bon, soweit gebucht
Datensicherung	TSE- und Fiskaldaten werden durch efsta (Anlage 3, Nr. 15) verschlüsselt im efsta-Cloud-Archiv in der EU gespeichert, für die gesetzliche Aufbewahrungsfrist von mindestens 10 Jahren.
Subunternehmer	Keine. efsta (Anlage 3, Nr. 15) handelt als eigener Verantwortlicher.

Anlage 2

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen

Zertifiziertes Informationssicherheits-Managementsystem (ISO/IEC 27001)

Die SoftTec GmbH betreibt ein nach ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem (ISMS). Die Wirksamkeit der Maßnahmen wird durch interne Audits sowie die jährlichen Überwachungsaudits der Zertifizierungsstelle überprüft.

Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

Bei der SoftTec GmbH wird der Schutz personenbezogener Daten im Rahmen des Möglichen und unter Berücksichtigung des Stands der Technik sowie der verfügbaren Ressourcen umgesetzt. Von Beginn an legen wir Wert darauf, Datenschutz und Sicherheit in die Gestaltung und Auswahl von Hardware, Software und Verfahren einzubinden (Privacy by Design und Privacy by Default). Dabei streben wir an, potenzielle Risiken für die Rechte und Freiheiten von Personen, soweit vorhersehbar, angemessen zu reduzieren.

Verpflichtung zur Vertraulichkeit und Sensibilisierung der Mitarbeiter

Mitarbeiter der SoftTec GmbH sind auf Vertraulichkeit verpflichtet und werden regelmäßig und mit Nachweis zu Informationssicherheit und Datenschutz geschult. Für Homeoffice, mobiles Arbeiten und die Nutzung privater Geräte gelten verbindliche Richtlinien, deren Kenntnisnahme dokumentiert wird.

Verwaltung und Entzug von Zugangs- und Berechtigungsrechten

Die an Mitarbeiter ausgegebenen Schlüssel, Zugangskarten oder Codes sowie die Berechtigungen zur Verarbeitung personenbezogener Daten werden bei ihrem Ausscheiden aus dem Unternehmen oder bei einem Wechsel der Zuständigkeiten überprüft und angepasst bzw. entzogen. Dadurch wird sichergestellt, dass nur autorisierte Personen Zugang zu sensiblen Bereichen und Daten haben.

Zutrittskontrolle

Sicherheitsmaßnahmen zum Schutz physischer und elektronischer Daten

Die Verarbeitung personenbezogener Daten bei der SoftTec GmbH erfolgt überwiegend elektronisch. Für den Fall, dass personenbezogene Daten in physischer Form vorliegen und eines speziellen Zutrittsschutzes bedürfen, wird dieser durch geeignete Maßnahmen wie den Verschluss in sicheren Schränken oder die Verwahrung in abschließbaren Räumen sichergestellt. Zusätzlich wird gewährleistet, dass Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, indem diese durch ein Chipkarten- und Transponder-Schließsystem geschützt sind. Diese Maßnahmen gewährleisten, dass nur befugte Personen Zugang haben und minimieren das Risiko eines unberechtigten Zugriffs.

Regelungen zum Zugang betriebsfremder Personen und externer Dienstleister: Betriebsfremde Personen dürfen die Räumlichkeiten der SoftTec GmbH grundsätzlich nur in Begleitung eines autorisierten internen Mitarbeiters betreten. Ausnahmen bestehen für externe Dienstleister, wie zum Beispiel Reinigungspersonal.

Überwachung und Schutz der technischen Einrichtungen

Zutritte werden protokolliert. Der Serverraum ist als Sicherheitsbereich nur für berechtigte Personen zugänglich und unter anderem durch eine unterbrechungsfreie Stromversorgung abgesichert.

Aufgeräumter Arbeitsplatz und Bildschirmsperren

Es gelten Vorgaben zu Clean Desk und Clean Screen. Bildschirme sperren sich nach einer festgelegten Zeit der Inaktivität automatisch.

Zugangskontrolle / Zugriffskontrolle

Verwendung personenbezogener Benutzeraccounts zur Zugriffsnachverfolgbarkeit

Mitarbeiter der SoftTec GmbH erhalten personenbezogene Benutzeraccounts. Jeder Zugang darf nur von der Person genutzt werden, der er zugewiesen ist. Dadurch sind Zugriffe auf Systeme und Anwendungen einer Person zuordenbar. Gemeinsam genutzte Zugänge sind nur in begründeten Ausnahmefällen, befristet und dokumentiert zulässig.

VPN-Einsatz zur Absicherung externer Zugriffe auf interne Systeme

Der Zugriff auf interne Systeme von außerhalb des Unternehmensnetzwerks erfolgt über eine verschlüsselte VPN-Verbindung. Datenträger und Unterlagen mit sensiblen Informationen werden sicher aufbewahrt.

Erhöhte Zugangssicherheit durch Zwei-Faktor-Authentifizierung (2FA)

Die Authentifizierung erfolgt standardmäßig mit Zwei-Faktor-Authentifizierung (2FA), soweit die eingesetzten Systeme dies unterstützen.

Berechtigungskonzept nach dem Prinzip der minimalen Rechte (Least Privilege Principle)

Zugriffsrechte werden rollen- und aufgabenbezogen nach dem Prinzip der minimalen Rechte (Need-to-know, Least Privilege) vergeben, geändert und entzogen. Privilegierte Rechte werden nur bedarfsbezogen vergeben; der Zugriff auf Quellcode ist rollenbasiert geregelt.

Passwortsicherheitsrichtlinien gemäß branchenüblichen Standards

Die SoftTec GmbH setzt Mindestanforderungen an die Passwortsicherheit um, die sich an branchenüblichen Standards orientieren.

Überwachung und anlassbezogene Protokollierung

Systeme und Endgeräte werden über Endpoint-Schutz und Monitoring auf auffällige Aktivitäten überwacht. Bei einem Sicherheitsvorfall oder dem Verdacht auf eine Verletzung des Schutzes personenbezogener Daten aktiviert die SoftTec GmbH eine erweiterte Protokollierung der Zugriffe auf die betroffenen Systeme, um den Sachverhalt aufzuklären.

Eingabekontrolle

Eingaben, Änderungen und Löschungen

Daten werden über personenbezogene Konten mit rollenbasierten Rechten eingegeben, geändert und gelöscht.

Weitergabekontrolle

Prüfung der Pseudonymisierung zur sicheren Datenverarbeitung

Die SoftTec GmbH prüft die Möglichkeit der Pseudonymisierung von personenbezogenen Daten, um, sofern technisch und organisatorisch machbar, das Risiko für betroffene Personen zu minimieren. Dabei wird der Einsatz von Pseudonymen erwogen, um direkte Identifikationsmerkmale zu reduzieren und gleichzeitig eine sichere Datenverarbeitung zu gewährleisten.

Verschlüsselung

Der Zugriff auf die Cloud-Hotelsoftware und der Datenaustausch mit angebundenen Plattformen erfolgen verschlüsselt (TLS). E-Mails werden transportverschlüsselt versendet, soweit der empfangende Server dies unterstützt.

Geregelte Informationsübermittlung

Informationen werden nur über freigegebene Kommunikations- und Austauschkanäle übermittelt. Für vertrauliche Informationen gelten Vorgaben zur Prüfung der Empfänger, zu Berechtigungen und zur getrennten Übermittlung von Zugangsdaten.

Auftragskontrolle

Auswahl und Überwachung von Subunternehmern

Subunternehmer werden risikobasiert ausgewählt. Bei Auftragsverarbeitung schließt die SoftTec GmbH AV-Verträge und fordert Nachweise zu den technischen und organisatorischen Maßnahmen an. Änderungen bei Lieferantendienstleistungen werden überwacht und bewertet. Weisungen des Auftraggebers werden in Textform festgehalten (§ 3.4).

Vorfallmanagement

Behandlung von Sicherheitsvorfällen

Die SoftTec GmbH verfügt über ein dokumentiertes Verfahren zur Erkennung, Bewertung und Behandlung von Sicherheitsvorfällen. Mitarbeiter melden beobachtete oder vermutete Ereignisse über einen festgelegten Meldeweg. Vorfälle werden erfasst, eingestuft und bis zum Abschluss nachverfolgt, Beweismaterial wird gesichert und Erkenntnisse fließen in Verbesserungen ein. Betroffene Auftraggeber werden nach § 5.1 informiert.

Verfügbarkeitskontrolle / Integrität

Betrieb in zertifizierten Rechenzentren

Die Produktivsysteme der Cloud-Produkte betreibt die SoftTec GmbH in nach ISO/IEC 27001 zertifizierten Rechenzentren in Europa (unter anderem Microsoft Azure, TERRA CLOUD, IONOS); ausgenommen ist der SoftTec Chatbot (Chatbase, USA, siehe Anlage 1). Interne Systeme werden zusätzlich in einem gesicherten Serverraum am Standort Sonthofen betrieben.

Kontrolliertes Backup- und Recoverykonzept zur Sicherstellung der Geschäftskontinuität

Die SoftTec GmbH verfügt über ein ständig kontrolliertes Backup- und Recoverykonzept, das sicherstellt, dass alle wichtigen Daten regelmäßig gesichert und im Falle eines Systemausfalls oder Datenverlusts schnell und vollständig wiederhergestellt werden können. Dieses Konzept schützt vor Datenverlust und gewährleistet die Geschäftskontinuität. Die Datensicherung erfolgt je Produkt:

- Cloud-Hotelsoftware (einschließlich Buchungsmaschine): minütliche Sicherung in Microsoft Azure, zeitpunktgenau wiederherstellbar. Tägliche Sicherungen werden einen Monat (30 bzw. 31 Tage), monatliche Sicherungen weitere 11 Monate aufbewahrt (insgesamt 12 Monate). Die Sicherungen werden bei Microsoft redundant gespeichert.
- hotlineCloud: tägliche Sicherung im Rechenzentrum der TERRA CLOUD in einem getrennten Brandabschnitt mit Replikation in ein zweites Rechenzentrum. Tägliche Sicherungen werden einen Monat (30 bzw. 31 Tage), monatliche Sicherungen weitere 11 Monate aufbewahrt (insgesamt 12 Monate).
- Lokal installierte hotline Hotelsoftware: Die Datensicherung liegt in der Verantwortung des Auftraggebers, sofern sie nicht als Leistung gebucht ist; dann erfolgt sie durch den Auftragnehmer über comtrance.

Verbindliche Verfügbarkeiten richten sich nach den Regelungen des Hauptvertrags.

Notfallvorsorge

Für Störungen und Notfälle hat die SoftTec GmbH Abläufe und Zuständigkeiten festgelegt.

Schutz vor Schadsoftware und Netzwerksicherheit

Endgeräte und Server sind durch Endpoint-Schutz mit zentralem Webschutz geschützt. Software wird regelmäßig aktualisiert. Netzwerkbereiche sind getrennt, insbesondere das interne Netz vom Gastzugang; Netzwerkkomponenten sind physisch geschützt.

Patch- und Schwachstellenmanagement

Die von außen erreichbaren Systeme werden regelmäßig automatisiert auf Schwachstellen geprüft. Erkannte Schwachstellen werden bewertet, nach ihrem Risiko priorisiert und bis zur Behebung nachverfolgt.

Sichere Softwareentwicklung

Sicherheitsanforderungen werden im gesamten Entwicklungszyklus berücksichtigt. Änderungen an Systemen und Anwendungen durchlaufen definierte Entwicklungs- und Freigabeprozesse mit Reviews und nachvollziehbarer Dokumentation; Sicherheitsprüfungen sind in Entwicklung und Abnahme integriert.

Gewährleistung des Zweckbindungs-/Trennungsgebotes

Trennung von Umgebungen und Mandanten

Die SoftTec GmbH trennt Entwicklungs-, Test-, Demo-, Beta- und Produktionsumgebungen und regelt Übergänge kontrolliert. Die Nutzung produktiver oder personenbezogener Daten in Testumgebungen ist beschränkt. Die Daten der Auftraggeber sind mandantengetrennt; bei hotlineCloud erhält jeder Auftraggeber einen eigenen Server.

Löschung

Löschung personenbezogener Daten

Personenbezogene Daten werden auf Weisung des Auftraggebers sowie nach Vertragsende gemäß § 5.2 gelöscht.

Löschung von Datenträgern und Geräten

Nicht mehr benötigte Informationen werden nach organisatorischen Vorgaben gelöscht. Externe Speichermedien sind nur mit Genehmigung zulässig. Geräte und Datenträger werden vor Entsorgung oder Wiederverwendung sicher gelöscht, neu aufgesetzt oder physisch vernichtet.

Anlage 3

Liste der bestehenden Subunternehmer nach Produkten

Die Subunternehmer sind nach Produkten geordnet. Die Subunternehmer unter „Für alle Produkte“ gelten für jeden Auftraggeber, die übrigen nur, soweit der Auftraggeber das jeweilige Produkt nutzt.

Nr.	Subunternehmer / Anschrift	Kontakt	Zweck	Verarbeitungsort
Für alle Produkte				
1.	STRATO GmbH Otto-Ostrowski-Straße 7 10249 Berlin	+49 (0) 30 / 3001460 impressum@strato.de www.strato.de	Hosting	EU
2.	IONOS SE Elgendorfer Str. 57 56410 Montabaur	+49 (0) 721 / 1705522 info@ionos.de www.ionos.de	Hosting (u. a. RESERVATE)	EU
3.	CHT GmbH & Co. KG Werner-von-Siemens-Str. 6 86159 Augsburg	+49 (0) 821 / 4504140 post@cht.de www.cht.de	Externe Datensicherung	Deutschland
4.	TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	privacy@teamviewer.com www.teamviewer.com	Fernwartung im Bedarfsfall	EU
5.	DEVWARE GmbH Güterstraße 20 42117 Wuppertal	+49 202 478269-0 info@devware.de www.devware.de	Externe Softwareentwicklung und IT-Dienstleistung	Deutschland
SoftTec Cloud Hotelsoftware				
6.	HERE Europe B.V. Kennedyplein 222-226 5611 ZT Eindhoven, Niederlande	+31 40 298 14 00 info@here.com www.here.com Datenschutz: privacy@here.com	PLZ-/Adresssuche in der SoftTec Cloud Hotelsoftware (Geocoding)	EU (Irland); bei schwerer regionaler Störung Ausweichen in die USA oder nach Singapur möglich, abgesichert durch EU-US Data Privacy Framework (Art. 45 DSGVO) bzw. Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
7.	Microsoft Ireland Operations, Ltd. One Microsoft Place, South County Business Park Leopardstown, Dublin 18, D18 P521, Irland	01806 / 672255 kunden@microsoft.com www.microsoft.com	Hosting und externe Datensicherung (Cloud-Hotelsoftware einschließlich Buchungsmaschine)	EU; Support-Zugriffe aus Drittländern möglich, abgesichert durch EU-US Data Privacy Framework (Art. 45 DSGVO) bzw. Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
8.	Brevo GmbH Köpenicker Str. 126 10179 Berlin	dpo@brevo.com www.brevo.com	E-Mail-Versand aus der Cloud-Hotelsoftware (Gästekommunikation)	EU (Hosting Frankreich/Belgien); Zugriffe aus Drittländern (USA, Indien) möglich, abgesichert durch Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) bzw. EU-US Data Privacy Framework (Art. 45 DSGVO)
8a.	chatlyn GmbH Renngasse 4/R4-4 1010 Wien, Österreich	support@chatlyn.com www.chatlyn.com	SMS-Versand aus der Cloud-Hotelsoftware (Gästekommunikation)	EU (Hosting Frankfurt, Deutschland)
hotline Hotelsoftware (lokal installiert) und Caesar Data				
9.	comtrance service GmbH In der Steele 35 40599 Düsseldorf	+49 (0) 211 271 59 20 info@comtrance.net www.comtrance.net	IT-Dienstleistung, Hosting und Datensicherung	Deutschland
hotlineCloud und Modul KassenSichV (Kassen-Middleware)				
10.	Ruthardt Systemhaus GmbH Stadionstr. 66 70771 Leinfelden-Echterdingen	+49 (0) 711 / 2526910 info@ruthardt-system.de www.ruthardt-system.de	Externe IT-Dienstleistung; Betrieb der Server für hotlineCloud und die Kassen-Middleware	Deutschland

Nr.	Subunternehmer / Anschrift	Kontakt	Zweck	Verarbeitungsort
11.	TERRA CLOUD GmbH (Unterauftragnehmer der Ruthardt Systemhaus GmbH) Hankamp 2, 32609 Hüllhorst	+49 (0) 5744 / 9440 support@terracloud.de terracloud.de	Hosting und externe Datensicherung	Deutschland
RESERVATE				
12.	Google Ireland Limited Gordon House, Barrow Street Dublin 4, D04 E5W5, Irland	+353 1 543 1000 www.google.com	Schutz vor automatisierten Buchungen (reCAPTCHA)	EU/USA (EU-US Data Privacy Framework, Art. 45 DSGVO)
SoftTec Payment (Cloud Hotelsoftware und RESERVATE)				
13.	Adyen N.V. Simon Carmiggeltstraat 6-50 1011 DJ Amsterdam, Niederlande	+49 30 30808105 germany@adyen.com www.adyen.com	Zahlungsabwicklung; Adyen handelt als eigener Verantwortlicher und ist zur Transparenz aufgeführt	EU (Speicherung nur in EU-Rechenzentren); Zugriffe aus Drittländern möglich, abgesichert durch Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
14.	Datatrans AG Kreuzbühlstrasse 26 8008 Zürich, Schweiz	www.datatrans.ch	Sichere Erfassung und Speicherung von Kreditkartendaten, z. B. als Buchungsgarantie; Datatrans handelt als eigener Verantwortlicher und ist zur Transparenz aufgeführt	Schweiz; Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO)
Modul KassenSichV (Fiskalisierung)				
15.	efsta IT Services GmbH Pachergasse 17 / Top 11 4400 Steyr, Österreich	+43 (0) 7252 93078-0 office@efsta.eu www.efsta.eu	Fiskalisierung und Belegarchivierung; efsta handelt als eigener Verantwortlicher und ist zur Transparenz aufgeführt	EU
SoftTec Chatbot				
16.	Chatbase Inc. 2261 Market Street STE 85690 San Francisco, CA 94114, USA	privacy@chatbase.co www.chatbase.co	Bereitstellung der Chatbot-Plattform	USA; abgesichert durch EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)