AXELROD

AUFTRAGSVERARBEITUNGSVERTRAG (AVV)
AXELROD AI ENGINE

VERSION 1.0

---

zwischen dem im Bestellformular genannten Kunden („Verantwortlicher“) und der Axelrod Labs, Inc., 1390 Market Street, Suite 200, PMB 17801953, San Francisco, CA 94102, USA („Auftragsverarbeiter“).

1 GEGENSTAND UND DAUER

1.1 Dieser AVV regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen bei der Erbringung des Dienstes „Axelrod AI Engine“ nach dem zwischen den Parteien geschlossenen Vertrag aus Bestellformular und AGB („Hauptvertrag“).

1.2 Er gilt für die Dauer des Hauptvertrags und darüber hinaus, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen besitzt.

1.3 Begriffe, die die Verordnung (EU) 2016/679 (DSGVO) definiert, haben in diesem AVV dieselbe Bedeutung.

2 ART UND ZWECK DER VERARBEITUNG

2.1 Der Auftragsverarbeiter verarbeitet die Daten ausschließlich, um den Dienst zu erbringen. Gegenstand, Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen beschreibt Anlage 1.

2.2 Der Auftragsverarbeiter verarbeitet die Daten nicht für eigene Zwecke, insbesondere nicht zum Training von KI-Modellen und nicht für Werbung. Technische Betriebsdaten des Dienstes wertet er nur anonymisiert aus; der Verantwortliche weist ihn an, die Daten dafür zu anonymisieren.

3 WEISUNGEN

3.1 Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Als Weisungen gelten der Hauptvertrag, dieser AVV, die Einstellungen, die der Verantwortliche und seine Nutzer im Dienst vornehmen, und Einzelweisungen in Textform.

3.2 Weisungen erteilen und empfangen die im Bestellformular genannten Ansprechpartner. Änderungen teilen die Parteien einander in Textform mit.

3.3 Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, weist er den Verantwortlichen unverzüglich darauf hin. Er darf die Ausführung aussetzen, bis der Verantwortliche die Weisung bestätigt oder ändert.

3.4 Ist der Auftragsverarbeiter nach dem Recht der Union oder eines Mitgliedstaats zu einer weiteren Verarbeitung verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.5 Einzelweisungen, die eine Anpassung der Standardleistung erfordern, sind nur verbindlich, wenn die Parteien sie in Textform vereinbart haben.

4 PFLICHTEN DES VERANTWORTLICHEN

4.1 Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und seiner Weisungen verantwortlich. Er sorgt für die Rechtsgrundlage, erfüllt die Informationspflichten gegenüber Gästen und Beschäftigten und wahrt die Rechte der betroffenen Personen. Machen Dritte wegen der Verarbeitung Ansprüche gegen den Auftragsverarbeiter geltend, stellt der Verantwortliche ihn davon frei, soweit sie auf einem Verstoß des Verantwortlichen gegen diesen AVV oder gegen geltendes Recht beruhen.

4.2 Der Verantwortliche bestimmt, auf welche Postfächer und Systeme der Dienst zugreift. Er stellt sicher, dass es sich bei Postfächern um Funktionspostfächer handelt, die nicht für private Kommunikation der Beschäftigten genutzt werden.

4.3 Der Verantwortliche beschränkt die Rechte der für den Dienst angelegten Benutzerkonten auf das Erforderliche.

4.4 Der Verantwortliche unterrichtet den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt, und nennt ihm einen Ansprechpartner für den Datenschutz. Er stellt dem Auftragsverarbeiter die Angaben bereit, die dieser für sein Verzeichnis nach Art. 30 Abs. 2 DSGVO benötigt.

5 SICHERHEIT DER VERARBEITUNG

5.1 Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die Anlage 3 beschreibt. Die Parteien sind sich einig, dass diese Maßnahmen bei Vertragsschluss ein angemessenes Schutzniveau bieten.

5.2 Er darf die Maßnahmen an den technischen Fortschritt anpassen und durch gleichwertige ersetzen, wenn das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen auf Anfrage mit.

6 VERTRAULICHKEIT

6.1 Der Auftragsverarbeiter setzt für die Verarbeitung nur Personen ein, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht nach dem Ende ihrer Tätigkeit fort.

6.2 Beschäftigte des Auftragsverarbeiters erhalten Zugriff auf Daten des Verantwortlichen nur, soweit sie ihn für Betrieb, Support oder Fehlerbehebung benötigen. Der Auftragsverarbeiter unterweist sie im Datenschutz.

7 UNTERAUFTRAGSVERARBEITER

7.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter nennt Anlage 2; sie gelten als genehmigt.

7.2 Will der Auftragsverarbeiter einen Unterauftragsverarbeiter hinzuziehen oder ersetzen, teilt er das dem Verantwortlichen mindestens 14 Tage vorher in Textform mit. Der Verantwortliche kann binnen 14 Tagen nach der Mitteilung aus konkreten datenschutzrechtlichen Gründen in Textform widersprechen. Widerspricht er nicht, gilt die Änderung als genehmigt.

7.3 Widerspricht der Verantwortliche, suchen die Parteien eine Lösung. Finden sie binnen 14 Tagen keine, kann jede Partei den Hauptvertrag und diesen AVV mit einer Frist von 30 Tagen kündigen.

7.4 Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich Datenschutzpflichten auf, die denen dieses AVV im Wesentlichen entsprechen. Verarbeitet ein Unterauftragsverarbeiter Daten in einem Drittland, gilt Ziffer 8.

7.5 Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter dem Verantwortlichen dafür wie für eigenes Verhalten.

7.6 Keine Unterauftragsverarbeiter sind Dienstleister, die der Auftragsverarbeiter für reine Nebenleistungen ohne Zugriff auf Daten des Verantwortlichen einsetzt, etwa für Telekommunikation oder Bürodienste.

8 INTERNATIONALE ÜBERMITTLUNGEN

8.1 Der Auftragsverarbeiter speichert und verarbeitet die Daten des Verantwortlichen ausschließlich in Rechenzentren in der EU oder im EWR. Das gilt auch für die Unterauftragsverarbeiter nach Anlage 2. Der Auftragsverarbeiter selbst hat seinen Sitz in den USA. Seine Mitarbeiter greifen von dort nur zu, soweit Betrieb und Support das erfordern. Sonst verarbeitet er die Daten außerhalb der EU und des EWR nur mit Zustimmung des Verantwortlichen in Textform.

8.2 Für Übermittlungen vom Verantwortlichen an den Auftragsverarbeiter vereinbaren die Parteien die Standardvertragsklauseln der Europäischen Kommission nach dem Durchführungsbeschluss (EU) 2021/914, Modul 2 (Verantwortlicher an Auftragsverarbeiter). Sie sind durch diesen Verweis Bestandteil des AVV. Die Parteien unterzeichnen dafür das Bestellformular; mit dieser Unterzeichnung gelten auch die Standardvertragsklauseln und ihre Anhänge als unterzeichnet. Dabei gilt:

KLAUSEL	FESTLEGUNG
KLAUSEL 7 (KOPPLUNGSKLAUSEL)	findet keine Anwendung
KLAUSEL 9 BUCHSTABE A	Option 2 (allgemeine schriftliche Genehmigung); Frist nach Ziffer 7.2 dieses AVV
KLAUSEL 11 BUCHSTABE A	die optionale Regelung zu einer unabhängigen Streitbeilegungsstelle ist nicht gewählt
KLAUSEL 13 UND ANHANG I.C	zuständig ist die für den Verantwortlichen zuständige Datenschutzaufsichtsbehörde

KLAUSEL	FESTLEGUNG
KLAUSEL 17	Option 1; es gilt das Recht der Bundesrepublik Deutschland
KLAUSEL 18 BUCHSTABE B	die Gerichte der Bundesrepublik Deutschland
ANHANG I.A	Datenexporteur ist der Verantwortliche, Datenimporteur der Auftragsverarbeiter; Kontaktdaten laut Bestellformular
ANHANG I.B	Anlage 1 dieses AVV; die Übermittlung erfolgt fortlaufend
ANHANG II	Anlage 3 dieses AVV
ANHANG III	Anlage 2 dieses AVV

8.3 Bei Widersprüchen zwischen den Standardvertragsklauseln und diesem AVV oder dem Hauptvertrag gehen die Standardvertragsklauseln vor.

8.4 An Unterauftragsverarbeiter in einem Drittland übermittelt der Auftragsverarbeiter Daten nur, wenn für das Drittland oder den Empfänger ein Angemessenheitsbeschluss gilt oder geeignete Garantien nach Art. 46 DSGVO bestehen, insbesondere Standardvertragsklauseln.

8.5 Verlangt eine Behörde eines Drittlands vom Auftragsverarbeiter die Herausgabe von Daten des Verantwortlichen, prüft er die Rechtmäßigkeit des Verlangens, schöpft zumutbare Rechtsbehelfe aus, gibt nur das rechtlich Unvermeidbare heraus und unterrichtet den Verantwortlichen, soweit ihm das nicht untersagt ist.

8.6 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die Informationen bereit, die dieser für die Bewertung der Übermittlung benötigt.

9 RECHTE BETROFFENER PERSONEN

9.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu erfüllen.

9.2 Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst.

9.3 Auf Weisung des Verantwortlichen sucht, berichtigt, löscht oder exportiert der Auftragsverarbeiter die bei ihm gespeicherten Daten einer betroffenen Person unverzüglich.

10 DATENSCHUTZVERLETZUNGEN UND UNTERSTÜTZUNG

10.1 Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden ist.

10.2 Die Meldung beschreibt, soweit bekannt, die Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl der Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen und vorgeschlagenen Maßnahmen und eine Kontaktstelle. Fehlende Angaben reicht der Auftragsverarbeiter nach, sobald sie vorliegen.

10.3 Der Auftragsverarbeiter ergreift unverzüglich die nötigen Maßnahmen, um die Verletzung einzudämmen und ihre Folgen zu mindern, und dokumentiert sie.

10.4 Er unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm vorliegenden Informationen bei dessen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Meldungen an die Aufsichtsbehörde, Benachrichtigungen betroffener Personen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen. Ob eine Melde- oder Benachrichtigungspflicht besteht, beurteilt der Verantwortliche.

10.5 Wendet sich eine Aufsichtsbehörde wegen der Verarbeitung an den Auftragsverarbeiter, unterrichtet er den Verantwortlichen unverzüglich, soweit ihm das nicht untersagt ist.

10.6 Unterstützung, die über die üblichen Auskünfte hinausgeht und nicht durch einen Verstoß des Auftragsverarbeiters veranlasst ist, kann er nach vorheriger Abstimmung angemessen berechnen.

11 LÖSCHUNG UND RÜCKGABE

11.1 Während der Laufzeit löscht der Auftragsverarbeiter Daten nach den in Anlage 1 genannten Fristen.

11.2 Nach dem Ende des Hauptvertrags gibt der Auftragsverarbeiter die Daten nach Wahl des Verantwortlichen heraus oder löscht sie. Erteilt der Verantwortliche keine Weisung, löscht der Auftragsverarbeiter die Daten 30 Tage nach Vertragsende. Sicherungskopien werden im regulären Turnus überschrieben, spätestens 7 Tage danach.

11.3 Von der Löschung ausgenommen sind Daten, die der Auftragsverarbeiter nach dem Recht der Union oder eines Mitgliedstaats aufbewahren muss, und Nachweise über die ordnungsgemäße Auftragsverarbeitung. Solche Nachweise bewahrt er in geschwärzter oder anonymisierter Form und längstens 30 Tage auf.

11.4 Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung in Textform.

11.5 Daten in den Postfächern und der Hotelsoftware des Verantwortlichen, einschließlich der dort abgelegten Ergebnisse, liegen in dessen Systemen und sind von der Löschung durch den Auftragsverarbeiter nicht erfasst.

12 NACHWEISE UND KONTROLLEN

12.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die nötig sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO und aus diesem AVV nachzuweisen.

12.2 Der Nachweis erfolgt in der Regel durch die aktuelle Beschreibung der Maßnahmen nach Anlage 3, die Beantwortung von Fragenkatalogen und die Prüfberichte und Zertifikate der Infrastruktur-Dienstleister nach Anlage 2.

12.3 Der Verantwortliche darf die Einhaltung selbst oder durch einen beauftragten Prüfer überprüfen, wenn er einen konkreten und begründeten Verdacht eines Verstoßes darlegt oder die Nachweise nach Ziffer 12.2 keine angemessene Überprüfung ermöglichen. Die Prüfung findet in der Regel aus der Ferne statt, anhand von Unterlagen, Gesprächen und Einsicht in die Systeme per Bildschirmübertragung.

12.4 Prüfungen kündigt der Verantwortliche mit angemessener Frist an. Sie finden zu den üblichen Geschäftszeiten statt und stören den Betrieb nicht mehr als nötig. Prüfer sind zur Vertraulichkeit zu verpflichten und dürfen nicht im Wettbewerb zum Auftragsverarbeiter

stehen. Der Auftragsverarbeiter darf Auskünfte beschränken, soweit das zum Schutz der Daten anderer Kunden, der Sicherheit oder seiner Geschäftsgeheimnisse nötig ist.

12.5 Jede Partei trägt ihre Kosten selbst. Für die zweite und jede weitere Prüfung in einem Vertragsjahr kann der Auftragsverarbeiter seinen Aufwand angemessen berechnen, es sei denn, die Prüfung ist durch einen festgestellten Verstoß veranlasst.

12.6 Bei Kontrollen durch Aufsichtsbehörden wirkt der Auftragsverarbeiter im erforderlichen Umfang mit.

13 HAFTUNG

13.1 Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO. Diese Haftung beschränkt der AVV nicht.

13.2 Im Verhältnis der Parteien zueinander gelten die Haftungsregeln des Hauptvertrags. Der Ausgleich untereinander richtet sich nach Art. 82 Abs. 5 DSGVO.

13.3 Klausel 12 der Standardvertragsklauseln bleibt unberührt; Haftungsbeschränkungen des Hauptvertrags gelten nicht, soweit sie ihr widersprechen.

14 LAUFZEIT UND KÜNDIGUNG

14.1 Die Laufzeit dieses AVV folgt der des Hauptvertrags. Eine ordentliche Kündigung allein des AVV ist ausgeschlossen.

14.2 Der Verantwortliche kann den Hauptvertrag und diesen AVV fristlos kündigen, wenn der Auftragsverarbeiter schwerwiegend gegen Datenschutzvorschriften oder diesen AVV verstößt, eine rechtmäßige Weisung nicht ausführt oder Kontrollen vertragswidrig verweigert.

14.3 Nach dem Ende des Hauptvertrags verarbeitet der Auftragsverarbeiter die Daten nur noch zur Abwicklung nach Ziffer 11.

15 SCHLUSSBESTIMMUNGEN

15.1 In Fragen des Schutzes personenbezogener Daten geht dieser AVV dem Hauptvertrag vor. Die Standardvertragsklauseln gehen diesem AVV vor.

15.2 Änderungen und Ergänzungen dieses AVV bedürfen der Textform; ein elektronisches Format genügt.

15.3 Sind Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder andere Maßnahmen Dritter gefährdet, unterrichtet er den Verantwortlichen unverzüglich und weist die Dritten darauf hin, dass die Verantwortung für die Daten beim Verantwortlichen liegt.

15.4 Ist eine Bestimmung dieses AVV unwirksam, bleibt er im Übrigen wirksam.

15.5 Es gelten Recht und Gerichtsstand des Hauptvertrags, soweit die Standardvertragsklauseln nichts anderes bestimmen.

15.6 Ansprechpartner für den Datenschutz beim Auftragsverarbeiter: Saman Sayahpour, saman@axelrod.com. Vertreter in der Union nach Art. 27 DSGVO: Prighter EU Rep GmbH, Schellinggasse 3, 1010 Wien, Österreich.

ANLAGE 1

BESCHREIBUNG DER VERARBEITUNG

GEGENSTAND	Bereitstellung der Axelrod AI Engine mit den Agenten, die der Verantwortliche bestellt hat. Die Agenten, ihre Aufgaben, die Betriebe und die angebundenen Systeme nennt das Bestellformular. Nennt es für einen Agenten weitere Daten oder Personengruppen, gelten diese zusätzlich.
ART DER VERARBEITUNG	Auslesen von Nachrichten und Daten aus den angebundenen Systemen des Verantwortlichen, etwa aus E-Mail-Postfächern und der Hotelsoftware (PMS); Abruf von Angaben über Schnittstellen oder Bildschirmansichten dieser Systeme; Übermittlung von Inhalten an KI-Modelle; Erzeugen von Entwürfen, Vorschlägen und Auswertungen und ihre Ablage in den Systemen des Verantwortlichen; Ausführen von Aktionen in diesen Systemen, soweit der Verantwortliche sie freigegeben hat; Speicherung, Protokollierung und Löschung
ZWECK	Unterstützung der Beschäftigten des Verantwortlichen bei den Aufgaben der bestellten Agenten, etwa bei der Bearbeitung von Gästeanfragen und Reservierungen
KATEGORIEN BETROFFENER PERSONEN	Gäste und anfragende Personen; Personen, die für andere buchen (Reisebüros, Firmenkunden, Assistenzen); mitreisende Personen; Ansprechpartner von Geschäftspartnern und Dienstleistern des Verantwortlichen; Beschäftigte des Verantwortlichen, die den Dienst nutzen oder in den verarbeiteten Inhalten genannt sind
ARTEN PERSONENBEZOGENER DATEN	Name und Anrede; Kontaktdaten (E-Mail-Adresse, Telefonnummer, Anschrift); Reisedaten (An- und Abreise, Zimmerart, Personenzahl, Rate, Sonderwünsche); Reservierungs- und Bestätigungsnummern, Mitgliedsnummern von Treueprogrammen; Angaben zu Firma oder Reisebüro; Inhalte von Nachrichten und ihren Anhängen; in den angebundenen Systemen sichtbare Gast- und Buchungsdaten; Nutzerkennungen, Freigaben und Änderungen der Beschäftigten; technische Protokolldaten
BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN	nicht vorgesehen. Sie können beiläufig in Nachrichten enthalten sein, etwa Hinweise auf Allergien oder Barrierefreiheit. Zahlungskartennummern benötigt der Dienst nicht; soweit er sie erkennt, schwärzt er sie.
HÄUFIGKEIT	fortlaufend während der Laufzeit des Hauptvertrags
SPEICHERDAUER BEIM AUFTRAGSVERARBEITER	Kopien von Nachrichten und Entwürfen: 30 Tage; Bildschirmansichten: 30 Tage; Verbindungsdaten des Relays (nur Metadaten): 14 Tage; Prüfprotokoll mit geschwärzten Inhalten: 30 Tage; Sicherungskopien: 7 Tage

ANLAGE 2

UNTERAUFTRAGSVERARBEITER

UNTERNEHMEN	LEISTUNG	VERARBEITETE DATEN	ORT DER VERARBEITUNG	GRUNDLAGE DER DRITTLANDÜBERMITTLUNG
Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109, USA	Datenbank, Relay, Webanwendung und Protokolle des Dienstes; Ablage des Worker-Zugangstokens; Zugangsrechner des Workers, falls der Auftragsverarbeiter ihn betreibt; KI-Modelle von Anthropic und OpenAI über Amazon Bedrock ohne Aufbewahrung der Inhalte	alle Daten nach Anlage 1	Frankfurt (Region eu-central-1); KI-Modelle in Regionen innerhalb der EU	Standardvertragsklauseln nach dem Auftragsverarbeitungs-vertrag von AWS

KI-Modelle nutzt der Auftragsverarbeiter nur über Amazon Bedrock in Regionen innerhalb der EU. Er nutzt dabei nur Modelle und Funktionen, die ohne Aufbewahrung der Inhalte arbeiten (Zero Data Retention). In jeder genutzten AWS-Region setzt er auf Kontoebene eine Richtlinie durch, die Anfragen blockiert, die damit unvereinbar sind. Die Hersteller der Modelle erhalten keine Daten des Verantwortlichen. Weder der Auftragsverarbeiter noch ein Unterauftragsverarbeiter nutzt die Daten zum Training von KI-Modellen.

Die Betreiber der angebundenen Systeme, etwa des E-Mail-Systems und des PMS, sind Dienstleister des Verantwortlichen und keine Unterauftragsverarbeiter des Auftragsverarbeiters.

ANLAGE 3

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1 VERTRAULICHKEIT

Zutrittskontrolle: Der Auftragsverarbeiter betreibt keine eigenen Rechenzentren. Die Daten liegen in Rechenzentren der Infrastruktur-Dienstleister nach Anlage 2, die den physischen Zutritt nach ihren geprüften Verfahren sichern.

Zugangskontrolle: Zugang zu Verwaltungs- und Produktivsystemen haben nur benannte Mitarbeiter mit persönlichen Konten. Alle Administrationszugänge sind mit Mehr-Faktor-Authentifizierung geschützt. Der Quellcode wird automatisch auf versehentlich abgelegte Zugangsdaten geprüft.

Zugriffskontrolle: Berechtigungen folgen dem Grundsatz der geringsten Rechte. Mitarbeiter greifen auf Kundeninhalte nur für Betrieb, Support und Fehlerbehebung zu.

Trennung: Die Daten verschiedener Kunden sind in der Datenbank durch zeilenbezogene Zugriffsregeln je Mandant getrennt (Row-Level Security). Auf Wunsch ist eine eigene Datenbank je Kunde möglich. Entwicklung und Produktion laufen in getrennten Umgebungen.

Datenminimierung und Schwärzung: Erkannte Zahlungskartennummern werden geschwärzt. Das Prüfprotokoll enthält geschwärzte Inhalte. Das Relay speichert nur Metadaten der Verbindungen.

Verschlüsselung: Daten werden ausschließlich über TLS übertragen und verschlüsselt gespeichert. Die Autorisierungstoken für angebundene Postfächer sind zusätzlich mit AES-256-GCM im Envelope-Verfahren verschlüsselt.

Zugangsdaten zu Kundensystemen: Passwörter für das PMS oder die Windows-Anmeldung speichert der Auftragsverarbeiter nicht; Anmeldung und Mehr-Faktor-Authentifizierung nehmen Mitarbeiter des Hotels vor. Der Postfachzugriff beruht auf einer delegierten Freigabe, die der Verantwortliche jederzeit widerrufen kann.

2 INTEGRITÄT

Weitergabekontrolle: Läuft der Worker auf einem Rechner im Hotel, baut er nur ausgehende HTTPS-Verbindungen zum Dienst auf; eingehende Verbindungen in das Netz des Hotels sind dann nicht erforderlich. Betreibt der Auftragsverarbeiter den Zugangsrechner selbst, greift dieser über einen gesicherten Fernzugang auf die Systeme des Hotels zu.

Eingabekontrolle: Ein nur fortschreibbares Prüfprotokoll hält Vorschläge des Dienstes, Freigaben durch Nutzer sowie ausgeführte und fehlgeschlagene Aktionen fest.

Sichere Entwicklung: Änderungen an der Produktivumgebung werden nur nach Freigabe eingespielt. Gegen manipulierte Eingaben in E-Mails (Prompt Injection) schützt der Aufbau des Dienstes. Im Entwurfsmodus hat ein Agent im Postfach kein Senderecht. Er legt nur Entwürfe ab, die ein Mitarbeiter des Hotels vor dem Versand prüft.

Menschliche Kontrolle: Im Entwurfsmodus versendet der Dienst keine Nachrichten und ändert keine Buchungen.

3 VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeit: Der Dienst lässt sich je Kunde sofort anhalten.

Wiederherstellbarkeit: Der Auftragsverarbeiter erstellt mindestens täglich verschlüsselte Sicherungskopien der Datenbank. Sie werden 7 Tage aufbewahrt. Die Wiederherstellung wird regelmäßig getestet.

Betrieb bei Ausfall: Nachrichten und Daten bleiben in den Systemen des Verantwortlichen und können dort von Hand bearbeitet werden.

4 VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG

Datenschutz-Management: Benannter Ansprechpartner für Datenschutz und Sicherheit; Verzeichnis der Verarbeitungstätigkeiten; regelmäßige Überprüfung der Zugriffsrechte und der Maßnahmen

Schwachstellen-Management: Automatisierte Sicherheitsprüfungen bei Softwareänderungen; regelmäßige Aktualisierung der eingesetzten Komponenten

Datenschutz durch Technikgestaltung: Entwurfsmodus als Voreinstellung, auf das Nötige beschränkte Zugriffsrechte, Schwärzung nicht benötigter Angaben.

Kontrolle der Dienstleister: Auswahl nach Sicherheitsnachweisen, Verträge zur Auftragsverarbeitung, Liste nach Anlage 2.

5 ORGANISATION

- Beschäftigte sind zur Vertraulichkeit verpflichtet und werden im Datenschutz unterwiesen.
- Geregelte Vergabe und Entziehung von Zugängen bei Eintritt, Wechsel und Austritt; verschlüsselte Arbeitsgeräte mit Bildschirmsperre.