resmio

Dieses Dokument bitte auf den Seiten 1 und 10 markierten Stellen ausgefüllt und unterschrieben an support@resmio.com zurücksenden.

Anlage zum Vertrag "Software-Überlassung auf Zeit" –

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag gem. Artikel 28 DSGVO

Zwischen

_____

(Name und Anschrift)

_____

(Anschrift)

- **Auftraggeber** -

und

resmio GmbH
Katzwanger Str. 150
Gebäude 1c
90461 Nürnberg

- **Auftragnehmer** -

über Auftragsverarbeitung i.S.D. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Software-Überlassungsvertrag auf Zeit in ihren Einzelheiten beschriebenen Auftragsverarbeitung („**AVV**“) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten („**Daten**“) des Auftraggebers verarbeiten.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus den Allgemeinen Geschäftsbedingungen des Auftragnehmers, die Teil jedes Vertrags sind und den nachfolgenden Bestimmungen ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Im Einzelnen sind die folgenden Daten Bestandteil der Datenverarbeitung:

- Vor- und Nachname
- E-Mail-Adresse
- Telefonnummer
- Angaben zur Reservierung (Datum und Uhrzeit der Reservierung; Anzahl der Gäste an einem Tisch)
- Inhaltliche Angaben zur Reservierung (Essenswünsche, Sitzplatzwünsche, sonstige Kommentare/Anmerkungen zur Reservierung)

Der Auftragnehmer stellt für den Business to Business Bereich eine Softwareanwendung („**Widget**“) im Rahmen einer Software as a Service („**SaaS**“) Lösung auf Zeit zur Verfügung. Mittels des auf der Website des Auftraggebers eingepflegten Widgets wird es dem Auftraggeber ermöglicht u.a. online Reservierungsanfragen von Gästen entgegenzunehmen. Eine Reservierungsanfrage eines Gastes über das Widget stellt ein

Angebot auf Abschluss eines Bewirtungsvertrags („**invitatio ad offerendum**“) zwischen dem Gast und dem Auftraggeber dar.

Der Auftragnehmer ist nicht Vertragspartei des Bewirtungsvertrags. Der Auftraggeber ist Vertragspartei des Bewirtungsvertrags und Verantwortlicher nach Art. 4 Nr. 7 DS-GVO („**Verantwortlicher**“).

Der Auftragnehmer stellt das Widget im Rahmen des SaaS, sowie externe Serverleistungen für den Auftraggeber zur Verfügung. Dadurch kann der Auftraggeber die im Rahmen der Anbahnung, Durchführung und Beendigung des Bewirtungsvertrags generierten personenbezogenen Daten verarbeiten. Der Auftragnehmer ist nach Art. 4 Nr. 8 DS-GVO Auftragsverarbeiter des Auftragnehmers.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

2. Anwendungsbereich, Verantwortlichkeit und Ort der Datenverarbeitung

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format („**Textform**“) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden („**Einzelweisung**“). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

2.3 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet vorwiegend in einem Mitgliedstaat der Europäischen Union („**EU**“) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum

(„**EWR**“) statt. Die Übermittlung personenbezogener Daten in ein Drittland erfolgt nach Maßgabe des Kapitels V der DS-GVO.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3.3 Der Auftragnehmer unterstützt, soweit vereinbart, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in den Artikeln 33 bis 36 DS-GVO genannten Pflichten.

3.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die

Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.6 Der Auftragnehmer gewährleistet seine Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

3.7 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

3.8 Daten, Datenträger sowie sämtliche sonstigen Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

3.9 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt Ziffer 3.9 entsprechend.

4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5. Anfragen betroffener Personen

5.1 Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

5.2 Soweit vom Leistungsumfang erfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer

Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

6.3 Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

6.4 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Ziffer 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1 Der Einsatz von Subunternehmern als weiteren Auftragsverarbeitern ist zulässig. Mit Unterzeichnung der AVV erteilt der Auftraggeber die Zustimmung zum Einsatz von Subunternehmern.

7.2 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesem Subunternehmer im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Die Vereinbarung mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

7.3 Zurzeit sind für den Auftragnehmer die in **Anlage 2** zu diesem AVV mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Europäischen Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Das der AVV zugrunde liegende Vertragsverhältnis wird seitens der Parteien als dokumentierte Weisung und schriftliche Genehmigung, personenbezogene Daten in ein Drittland zu übermitteln, betrachtet.

7.4 Vor jeder Übermittlung personenbezogener Daten in ein Drittland, prüft der Auftragnehmer, ob die Einhaltung des EU-Datenschutzniveaus sichergestellt werden kann. Stützt der Auftragsverarbeiter des Auftragnehmers die Übermittlung auf einen Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DS-GVO) oder geeignete Garantien (Art. 46 DS-GVO), prüft der Auftragnehmer, ob diese im konkreten Fall ein angemessenes Schutzniveau gewährleisten. Ergibt die Prüfung, dass zusätzliche Maßnahmen erforderlich sind, bemüht sich der Auftragnehmer die in dieser Hinsicht erforderlichen Maßnahmen einzuhalten, indem der Kontakt zu Subdienstleistern gesucht wird, um zusätzliche Garantien zu erlangen.

7.5 Im Falle des Einsatzes eines weiteren Auftragsverarbeiters im Drittland bemüht sich der Auftragnehmer mit jedem weiteren Auftragsverarbeiter die Standardvertragsklauseln bzw. Standarddatenschutzklauseln der EU-Kommission gemäß Art 46 Abs. 2 DS-GVO abzuschließen. In jedem Fall ist der Auftragnehmer bemüht, die Vorgaben des Art 46 Abs. 2 DS-GVO zu beachten.

7.6 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

8. Geheimhaltung

8.1 Die Vertragsparteien sind verpflichtet, die ihnen unter diesem Vertrag von der jeweils anderen Partei zugänglich gemachten Informationen sowie Kenntnisse, die sie bei dieser Zusammenarbeit über Angelegenheiten – etwa technischer, kommerzieller oder organisatorischer Art – von der jeweils anderen Vertragspartei erlangen, vertraulich zu behandeln und während der Dauer sowie nach Beendigung dieser Vereinbarung ohne die vorherige schriftliche Einwilligung der betroffenen Partei nicht zu verwerten

oder zu nutzen oder Dritten zugänglich zu machen. Eine Nutzung dieser Informationen ist allein auf den Gebrauch zur Durchführung dieses Vertrages beschränkt.

8.2 Diese Vertraulichkeitsverpflichtung gilt nicht für Informationen, die

- bei Vertragsabschluss bereits allgemein bekannt waren oder
- nachträglich ohne Verstoß gegen die in diesem Vertrag enthaltenen Verpflichtungen allgemein bekannt wurden.

8.3 Die Vertragspartner legen die von ihnen eingegangenen Verpflichtungen zur Geheimhaltung und zum Datenschutz auch allen Personen oder Gesellschaften auf, die von ihnen im Rahmen der Zusammenarbeit beauftragt werden.

9. Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

10. Informationspflichten, Schriftformklausel, Rechtswahl

10.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutz-Grundverordnung liegen.

10.2 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

10.4 Es gilt deutsches Recht.

10.5 Gerichtsstand ist der Sitz des Auftragnehmers in Nürnberg.

11. Salvatorische Klausel

11.1 Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

11.2 An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

11.3 Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

12. Gegenzeichnung

Auftraggeber

_____

Vor- und Zuname,
Titel

_____ _____

(Unterschrift Auftraggeber) (Ort, Datum)

resmio GmbH als **Auftragnehmer**

Michael Schade,
Geschäftsführer resmio GmbH

_____ Nürnberg, XX.XX.202X

(Unterschrift Auftragnehmer) (Ort, Datum)

Es folgen zwei (2) Anlagen:

Anlage 1: Technische und organisatorische Massnahmen

Anlage 2: Eingesetzte Unterauftragsverarbeiter des Auftragnehmers

ANLAGE 1

Technische und organisatorische Maßnahmen der Datensicherheit gemäß

ART. 32 ABS. 1 LIT. B DS-GVO

Im Rahmen des täglichen Ablaufs der resmio GmbH sind die folgenden beschriebenen technischen und organisatorischen Maßnahmen nach der Datenschutz Grundverordnung getroffen worden. Diese Maßnahmen spielen den aktuellen Stand wieder. Sie unterliegen dem technischen Fortschritt und der Weiterentwicklung.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Zutrittskontrollsystem:

- Zutritt zu den Büroräumen von resmio erfolgt nur mit Schlüssel.
- Alle Dienste werden bei externen Anbietern gehostet. Das API-Backend und die Datenbank werden von einem externen Anbieter mit angemessener Benutzerkontrolle gehostet, die den Zugriff durch Dritte verhindert.

- Kunden, Mitarbeitern ohne Zugriffsberechtigung, Externe, Lieferanten und Reinigungskräfte haben demnach keinen Zutritt zum Serverraum, da dieser extern ausgelagert ist und dort verwaltet wird.

Zugangskontrolle, hier insbesondere die Datenträgerkontrolle

Benutzerverwaltung:

- Angemessene Zugangskontrollen wurden in die Software implementiert, um sicherzustellen, dass Benutzer (Restaurantbesitzer, Kellner, ...) nicht auf die Daten anderer Benutzer zugreifen können.

Kennwörter:

- Bei Ausscheiden eines Mitarbeiters werden seine personalisierten Accounts gesperrt.

Speicherkontrolle

Die Speicherkontrolle soll verhindern, dass Unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können.

- Festlegung von Berechtigungen in den IT-Systemen erfolgt von den Verantwortlichen der Systeme.

Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können.

- Alle Personen haben Vereinbarungen unterzeichnet, um die Vertraulichkeit von Informationen und Daten zu gewährleisten. Externes Personal („Freelancer“) hat keinen Zugang zu Daten aus Produktionssystemen.
- Alle externen Dienstleistungsanbieter haben entsprechende DPAs (Data Processing Agreements) unterzeichnet, um den Schutz der Daten zu gewährleisten.
- Sperrung von Berechtigungen ausscheidender Mitarbeiter erfolgt, wenn es ausscheidende Mitarbeiter gibt.
- Einsatz von Verschlüsselungs-Technologie bisher nur auf der Webseite. Transport Layer Security (**TLS**, englisch für Transportschichtsicherheit), weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (**SSL**), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet, erkennbar durch https, anstatt http in der URL.

Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

- Festlegung von Berechtigungen in den IT-Systemen
- Verwaltung der Rechte durch Systemverantwortliche
- Anzahl der Systemverantwortlichen ist auf das „Notwendigste“ reduziert
- Angemessene Zugangskontrollen wurden in die Software implementiert, um sicherzustellen, dass Benutzer (Restaurantbesitzer, Kellner, ...) nicht auf die Daten anderer Benutzer zugreifen können.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Übertragungskontrolle

Die Übertragungskontrolle soll gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- Die Benutzer werden nach dem Prinzip der geringsten Privilegien eingeschränkt. Das Recht, Daten zu ändern, wird nur dem internen IT-Personal gewährt. Kein externes Personal („Freelancer“) hat Zugriff auf Daten aus Produktionssystemen.

Transportkontrolle

Die Transportkontrolle soll gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

- Die Webseite ist verschlüsselt (TLS/SSL-Zertifikat)

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Wiederherstellbarkeit

Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- Das System ist auf der Cloud-Infrastruktur von Heroku aufgebaut.

- Heroku hat eine hochverfügbare Infrastruktur.

- Es gibt automatische Backups, die so konfiguriert sind, dass alle Daten täglich gesichert werden.

  Das Back-Up ist verschlüsselt und sichert automatisch täglich; Back-Up Varianten laufen autark und unabhängig vom Server und der serverseitigen Sicherung. Für den Fall, dass die Sicherung auf dem Server nicht erfolgt oder der Server ausfällt, können die Daten wiederhergestellt werden.

  - Vorhaltezeiten/Aufbewahrung: 4 Tage

Zuverlässigkeit

Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- Unabhängig voneinander funktionierende Systeme, die die Wiederherstellung der Daten ermöglichen.
- Automatisierte Meldung von Fehlfunktionen

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

- Alle Dienste werden bei externen Anbietern gehostet. Das API-backend und die Datenbank werden von einem externen Anbieter mit angemessener Verfügbarkeitskontrolle gehostet.
- Heroku nutzt automatische Branderkennungs- und -bekämpfungsanlagen sowie Rauchmeldesensoren in allen Rechenzentrumsumgebungen, mechanischen und elektrischen Infrastrukturräumen, Kühlräumen und Generatorausrüstungsräumen.

- Die Stromversorgungssysteme des Rechenzentrums von Heroku sind so ausgelegt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs 24 Stunden am Tag und sieben Tage in der Woche gewartet werden können. Unterbrechungsfreie Stromversorgungseinheiten stellen bei einem Stromausfall die Notstromversorgung für kritische und wesentliche Lasten in der Einrichtung sicher. Rechenzentren verwenden Generatoren, um die Notstromversorgung für die gesamte Einrichtung zu gewährleisten.

- Heroku nutzt eine Klimatisierung, um eine konstante Betriebstemperatur für Server und andere Hardware aufrechtzuerhalten, wodurch eine Überhitzung verhindert und die Möglichkeit von Betriebsausfällen verringert wird.

- Es erfolgt durch den Head of IT, Paval Goltsev**,** ein Monitoring des Systems.

  Monitoring ist die Überwachung von Vorgängen. Es ist ein Überbegriff für alle Arten von systematischen Erfassungen (Protokollierungen), Messungen oder Beobachtungen eines Vorgangs oder Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme.

  Eine Funktion des Monitorings besteht darin, bei einem beobachteten Ablauf oder Prozess festzustellen, ob dieser den gewünschten Verlauf nimmt und bestimmte Schwellenwerte eingehalten werden, um andernfalls steuernd eingreifen zu können. Monitoring ist deshalb ein Sondertyp des Protokollierens.

  Das Monitoring erfolgt mit der Software Cronitor, Uptime Robot, Heroku, Coralogix und Sentry.

  Mithin ist eine externe Überwachung des Systems durch Heroku möglich und regelmäßig durchzuführen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit d DS-GVO; Art.25 Abs. 1 DS-GVO)

Datenschutz-Datensicherheit

Datenschutz und Datensicherheit gehören zu den wichtigsten Prämissen. Sämtliche Maßnahmen unterliegen einer turnusgemäßen Überwachung, damit der Stand der Technik gewährleistet ist.

Datenschutzrechtliche Voreinstellungen (Art. 25 Abs. 2 Datenschutz Grundverordnung)

Es ist gewährleistet, dass nur solche personenbezogenen Daten erhoben werden, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Kontrolle der Auftragsverarbeiter

Mit den einzelnen Auftragsverarbeitern der resmio GmbH werden separate Vereinbarungen geschlossen. Es werden hier keine standardisierten Verträge abgezeichnet. Die Auftragsverarbeitung erfolgt unter Berücksichtigung des besonderen Zuschnitts der resmio GmbH und insbesondere im Hinblick auf die IT-kritischen Infrastrukturen.

ANLAGE 2

Eingesetzte Unterauftragsverarbeiter des Auftragnehmers

(Stand: April 2024)

Die Zustimmung zum Einsatz der unten genannten Unterauftragsverarbeiter für die genannten durchzuführenden Tätigkeiten wird erteilt, sofern die datenschutzrechtlichen Voraussetzungen entsprechend dieser Vereinbarung auch in diesem Vertragsverhältnis (Unterauftragsverarbeiter-AVV) eingehalten werden.

Name Unterauftags-verarbeiter	**Durchzuführende Tätigkeit(en)**	**Geschäfts-führung**	**Adresse**
Adyen N.V.	Zahlungsdienstleistungen	Pieter van der Does	Simon Carmiggeltstraat 6-50, 1011 DJ Amsterdam, Niederlande
Stripe Inc.	Zahlungsdienstleistungen	Patrick Collision	510 Townsend Street, San Francisco, CA 94103, USA

Amazon Web Services	Bedarfsgerechte Bereitstellung von Cloud-Ressourcen für die Auslieferung von Inhalten (Content-Delivery-Netzwerk) unseres SaaS-Angebots Ergänzender Nachtrag zum *Data Processing Addendum* seitens AWS mit zusätzlichen Garantien: https://d1.awsstatic.com/Supplementary_Addendum_to_the_AWS_GDPR_DPA.pdf	Jeff Bezos	410 Terry Avenue North, Seattle WA 98109, United States
GetResponse	E-Mail-Marketing, Newsletter-Erfolgsmessung, Webanalyse	Simon Grabowski	Arkonska 6/A3, 80-387 Gdansk, Polen
Intercom	Bereitstellung eines Live-Chat-Dienstes innerhalb der Webapplikation für Supportanfragen von Kunden	Eoghan McGabe	55 2nd Street, 4th floor, San Francisco, CA 94105, USA
Google LLC	Website & Application Analytics (via Google Analytics / Google Tag Manager), interne Kommunikation über E-Mail und GSuite Office	Sundar Pichai	1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA
Odoo S.A.	Bereitstellung eines Cloud-betriebenen CRM-Systems für die Verwaltung von Vertrieb, Marketing, Kundenbetreuung und Buchhaltung	Sébastien Bruyr	Chaussée de Namur 40, 1367 Ramillies, Belgien

rapidmail GmbH	Versendung von informellen, nicht-werblichen E-Mail-Newslettern an Kunden des Auftraggebers	Sven Kummer	Augustinerplatz 2, 79098 Freiburg, Deutschland
Sendgrid Inc.	Bereitstellung eines Service für den automatisierten Versand von E-Mail-Benachrichtigungen aus dem System (z.B. Buchungsbenachrichtigungen an Gastronomen / Kellner)	Sameer Dholakai	1801 California Street, Suite 500, Denver, Colorado 80202, USA
Salesforce.com Inc.	Hosting / Datenspeicherung der Webapplikation Erfassung und Protokollierung von Software-Fehlern zu Analyse- und Optimierungszwecken (*Sentry*) Zwischenspeicherung der Daten zur Bewältigung rechenintensiver Hintergrundprozesse (*CloudAMQP*) - Bereitstellung einer generellen Login-Lösung (*Coralogix*)	Adam Gross	The Landmark @ One Market Street, Suite 300**,** San Francisco, CA 94105, USA
Vonage B.V.	Automatisierter SMS-Versand, z.B. als Service-Leistung für Benachrichtigungen über eingehende Reservierungen	David Jaarsma	Prins Bernhardplein 200, 1097 JB, Amsterdam, Niederlande