Vertrag zur Verarbeitung personenbezogener Daten im Auftrag nach Art 28 DSGVO

1. Gegenstand und Dauer des Vertrags

1. Dieser Auftragsverarbeitungs-Vertrag (der „Vertrag“) regelt die Verarbeitung der personenbezogenen Daten, die der Auftragnehmer bei der Erbringung seiner Leistungen für den Auftraggeber im Rahmen eines gesonderten Vertrages (der „Hauptvertrag“) verarbeitet. Gegenstand des Hauptvertrages die Beauftragung des Auftragnehmers durch den Auftraggeber mit der Bereitstellung der SaaS-Anwendung und der dazugehörigen Smartphone-App („Plattform“). Im Rahmen dieses Auftrages ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für welche der Auftraggeber der Verantwortlicher im Sinne der EU-Datenschutz-Grundverordnung („DSGVO“) ist.
2. Der vorliegende Vertrag ist den Allgemeinen Geschäftsbedingungen des Auftragnehmers als **Vertrag zur Auftragsverarbeitung (Anlage III)** beigefügt und gilt als deren integrierender Bestandteil.
3. Aus datenschutzrechtlicher Sicht sind die gegenständlichen Verarbeitungstätigkeiten als Verarbeitung im Auftrag des Auftraggebers im Sinne von Art 4 Z 2 und Art 28 DSGVO zu qualifizieren und kommt daher dem Auftragnehmer aus datenschutzrechtlicher Sicht die Rolle des Auftragsverarbeiters zu. Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Leitungen nach Maßgabe des Art 28 DSGVO ordnungsgemäß durchzuführen.
4. Dieser Vertrag regelt die datenschutzrechtlichen Maßnahmen im Sinne von Art 28 DSGVO sowie die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der datenschutzrechtlichen Anforderungen.
5. Der Vertrag tritt mit Unterfertigung des Hauptvertrages in Kraft. Die Vertragsdauer und Kündigungsmöglichkeiten richten sich nach dem Hauptvertrag.

2. Kategorien der verarbeiteten Daten und betroffene Personen

1. Die verarbeiteten Datenkategorien sowie die Kategorien der durch die Verarbeitung betroffenen Personen sind in **Anlage 1** erfasst.
2. Es werden keine besonderen Kategorien personenbezogener Daten im Sinne des Art 9 Abs 1 DSGVO verarbeitet.

3. Pflichten des Auftragnehmers

3.1. Allgemeines

1. Der Auftragnehmer erhebt, speichert und verarbeitet dazu personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Der Auftraggeber bleibt im datenschutzrechtlichen Sinne Verantwortlicher.
2. Der Auftragnehmer ist nicht berechtigt, die Daten ohne in Textform erteilte Genehmigung durch den Auftraggeber für eigene Zwecke zu verwenden oder an Dritte zu übermitteln.
3. Der Auftragnehmer verarbeitet personenbezogene Daten im Rahmen des Auftrags ausschließlich innerhalb der Europäischen Union bzw. innerhalb des Europäischen Wirtschaftsraumes, sofern nicht in **Anlage 3** Abweichendes geregelt ist.

3.2. Weisungsgebundenheit

1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Bestimmungen dieses Vertrags und auf dokumentierte Weisung des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
2. Weisungen werden grundsätzlich im Hauptvertrag vereinbart. Weitere bzw nachträgliche Weisungen können vom Auftraggeber in dokumentierter Weise erteilt werden, wobei hierfür die Textform, und daher auch die elektronische Form (zB per E-Mail ohne elektronische Signatur) genügt. Mündliche Weisungen bestätigt der Auftragnehmer unverzüglich zumindest in Textform.
3. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten. Es obliegt daher dem Auftraggeber, seine Weisung gegebenenfalls zu korrigieren. Der Auftragnehmer hat das Recht, die Umsetzung der Weisung so lange auszusetzen, bis sie vom Auftraggeber abgeändert wurde, sodass sie rechtskonform ist.
4. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Der Auftraggeber und Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

3.3. Dokumentationspflicht

1. Der Auftragnehmer führt ein Verarbeitungsverzeichnis gemäß Art 30 Abs 2 DSGVO.
2. Änderungen des Verarbeitungsgegenstandes sind gemeinsam mit dem Auftraggeber abzustimmen und in Textform festzulegen.

3.4. Vertraulichkeit

1. Der Auftragnehmer ist verpflichtet, im Zuge der Datenverarbeitung neben besonderen gesetzlichen Verschwiegenheitspflichten das Datengeheimnis zu wahren.
2. Der Auftragnehmer gewährleistet, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.
3. Die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen bleibt auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

3.5. Technische und organisatorische Maßnahmen

1. Der Auftragnehmer garantiert die Sicherheit und daher Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäß Art 32 DSGVO. Der Auftragnehmer hat in diesem Sinn alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 ff DSGVO ergriffen. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich in **Anlage 2**. Der Auftragnehmer verpflichtet sich, dabei den Stand der Technik, die Art, den Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art 32 Abs 1 DSGVO berücksichtigt zu haben. Der Auftragnehmer versichert, dass mit den Maßnahmen nach **Anlage 2** ein Sicherheitsniveau gewährleistet ist, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten gerecht wird.
2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen,

soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

3.

3.6. Betroffenenrechte

1. Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zuständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen.
2. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, Einschränkung der Verarbeitung sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann, unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen von Betroffenenrechten und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Dies schließt auch die Unterstützung bei der Erfüllung der Rechte auf Einschränkung der Verarbeitung, sowie die Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung ein.
3. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 33 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.
4. Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarte Kontaktperson erteilt werden.
5. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen. Der Auftraggeber benennt hierfür einen für den Datenschutz zuständigen Ansprechpartner.
6. Werden dem Auftragnehmer Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt, so unterrichtet er den Auftraggeber unverzüglich und trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.
7. Der Auftragnehmer teilt dem Auftraggeber unverzüglich - spätestens aber binnen 48 Stunden ab Kenntnis - Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art 33 und Art 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art 33 und 34 DSGVO angemessen zu unterstützen (Art 28 Abs 3 Satz 2 lit f DSGVO). Meldungen nach Art 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

3.7. Einsichts- und Kontrollrechte

1. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht zur Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der

Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

2. Der Auftragnehmer ermöglicht vorangemeldete Überprüfungen zu Geschäftszeiten durch einen unabhängigen Dritten. Solche Überprüfungen werden in einer Art durchgeführt, die den Geschäftsbetrieb des Auftragnehmers nicht stören. Die Kosten, die durch solche Überprüfungen anfallen, werden zwischen Auftraggeber und Auftragnehmer aufgeteilt oder je nach Fall abgesprochen. Sollte ein Härtefall eintreten, der eine Überprüfung ohne vorherige Anmeldung erfordert, sind die Kosten vollständig vom Auftraggeber zu tragen. Dem Auftragnehmer steht für alle Leistungen in Zusammenhang mit der Unterstützung von Überprüfungen ein angemessenes Entgelt zu.

3. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

4. Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht umfasst sind Nebenleistungen, die der Auftragnehmer zB als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Der Auftragnehmer ist berechtigt, Unterauftragnehmer (Subauftragsverarbeiter) zur unmittelbaren Erfüllung der Dienstleistung zu beauftragen. Die zum Zeitpunkt des Abschlusses dieser Vereinbarung beauftragten Unterauftragnehmer sind in **Anlage 3** aufgeführt. Die geplante Beauftragung weiterer Unterauftragnehmer ist dem Auftraggeber vorab in Textform anzuzeigen. Der Auftraggeber kann der geplanten Beauftragung widersprechen. Erhebt der Auftraggeber innerhalb von 30 Tagen keinen Einspruch, so gilt die Beauftragung als genehmigt.
3. Bei Erhebung eines Einspruchs nach Punkt 4.2 erhält der Auftragnehmer das Recht, den Vertrag mit sofortiger Wirkung in Schriftform oder Textform durch eingeschriebenen Brief an hotelkit GmbH, Marie-Andeßner-Platz 1, 5020 Salzburg oder durch E-Mail an info@hotelkit.net zu kündigen.
4. Beauftragt der Auftragnehmer einen Unterauftragnehmer, so hat er mit diesem den erforderlichen Vertrag zur Auftragsverarbeitung gemäß Art 28 Abs 4 DSGVO abzuschließen. Dabei ist sicherzustellen, dass der Unterauftragnehmer dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund der vorliegenden Vereinbarung obliegen.
5. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers.

5. Haftung

1. Die Haftung beider Parteien ist in den AGB zum Hauptvertrag geregelt.
2. Dessen ungeachtet haftet der Auftraggeber dem Auftragnehmer für die Rechtmäßigkeit aller erteilten Weisungen und stellt ihn hinsichtlich aller aus der Befolgung einer Weisung resultierenden Schäden und Nachteile klag- und schadlos.

6. Verfahren nach Beendigung der Verarbeitungsleistungen

1. Nach Abschluss der Verarbeitung, spätestens nach Beendigung des Vertrages, hat der Auftragnehmer sämtliche in seinem Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten personenbezogenen oder sonstigen vertraulichen Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen und/oder in Abstimmung mit dem Auftraggeber datenschutzgerecht zu vernichten oder sicher zu löschen. Diese Verpflichtung gilt in gleichem Maße auch für eventuell beauftragte Unterauftragnehmer. Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismäßig hohen Aufwand verursachen würde, sowie Kopien, die zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind. Personenbezogene Daten sind jedoch stets zu löschen; falls dies nicht möglich ist, müssen diese anonymisiert werden.

2. Für diese Daten ist die Verarbeitung gem Art 18 DSGVO einzuschränken. Die Daten dürfen durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden und sind nach dem Ablauf der Aufbewahrungsfristen unverzüglich sicher zu löschen. Der Auftraggeber ist über Art und Umfang dieser gespeicherten Daten zu unterrichten. Der Auftragnehmer kann diese Daten zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.
3. Der Auftragnehmer hat dem Auftraggeber nach Beendigung des Vertrages die sichere Löschung bzw die sichere Vernichtung aller in seinem Besitz befindlichen Unterlagen in Textform zu bestätigen.

7. Ansprechpartner

Auf Seiten des Auftragnehmers werden folgende Ansprechpartner benannt:

Weisungsempfänger beim Auftragnehmer:
Marius Donhauser, Geschäftsführender Gesellschafter
E-Mail-Adresse: marius.donhauser@hotelkit.net

Ansprechpartner Datenschutz:
Ing. Mag. Jürgen Hutsteiner, CIPP/E
E-Mail-Adresse: dataprivacy@hotelkit.net

Der Auftraggeber wird dem Auftragnehmer eine weisungsberechtigte Person sowie einen Ansprechpartner für Datenschutz im Rahmen des Onboardings bekannt geben.

8. Schlussbestimmungen

1. Ausschließlicher Gerichtsstand ist A-5020 Salzburg. Soweit als nach zwingendem Recht zulässig, gilt ausschließlich österreichisches Recht unter Ausschluss der Verweisungsnormen des IPRG sowie des UN-Kaufrechtsübereinkommens (BGBl 1988/96).
2. Allfällige bereits bestehende datenschutzrechtliche Vereinbarungen der Vertragsparteien werden mit Inkrafttreten dieses Vertrages einvernehmlich außer Kraft gesetzt.
3. Sollte eine Bestimmung dieses Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, berührt dies nicht die Wirksamkeit oder Durchführbarkeit der übrigen Bestimmungen. Die unwirksame oder undurchführbare Bestimmung wird durch eine wirksame oder durchführbare Bestimmung ersetzt, die in ihrem wirtschaftlichen Gehalt der unwirksamen oder undurchführbaren Bestimmung möglichst nahe kommt; dasselbe gilt entsprechend für Lücken in diesem Vertrag.
4. Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Von diesem Formerfordernis kann seinerseits nur durch Vereinbarung in Textform abgewichen werden. Mündliche Nebenabreden zu diesem Vertrag bestehen nicht.
5. Treten Änderungen in der Gesetzeslage ein, welche die Wirksamkeit des Vertrages betreffen, so verpflichten sich die Parteien, gemeinsam auf eine rechtswirksame Änderung dieses Vertrages hinzuwirken.
6. Die **Anlagen 1 bis 3** bilden integrierende Bestandteile des Vertrages. Sofern diese angepasst werden, sind sie dem Vertrag hinzuzufügen und ersetzen die jeweils alte Anlage.

Anlage 1: Kategorien verarbeiteter Daten und betroffene Personengruppen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Auftraggeber (siehe Auftraggeberdaten);
- Mitarbeiter des Auftraggebers und sonstige vom Auftraggeber zur Nutzung der Plattform berechtigte, mitarbeiter-ähnliche Personen (siehe Mitarbeiterdaten);
- Lieferanten des Auftraggebers (siehe Lieferantendaten);
- Kunden des Auftraggebers und sonstige Personen in Einrichtungen des Auftraggebers sowie sonstige Betroffene (siehe Kundendaten).

Die nachfolgend aufgelisteten Kategorien von personenbezogenen Daten werden im Rahmen der Auftragsverarbeitung durch den Auftragnehmer verarbeitet:

Teil A: Allgemeine Daten

Dieser Teil erfasst alle personenbezogenen Daten, die innerhalb des Netzwerkes bereichsübergreifend verwendet werden können. Für manuell erfasste Felder erfolgt kein technischer Zwang zur Erfassung, soweit nicht anders angegeben. Eine Erfassung kann jedoch durch den Auftraggeber im Rahmen betrieblicher Vereinbarungen gefordert werden.

Mitarbeiterdaten

Bezeichnung	**Beschreibung**	**Verwendungszweck**
Name	Vorname und Nachname des Betroffenen	Eindeutige Identifizierung des Nutzers in der Kommunikation innerhalb des Mitarbeiterkreises des Auftraggebers
E-Mail-Adresse[1]	Berufliche Emailadresse des Mitarbeiters	- Zustellen von Benachrichtigungen - Zurücksetzen von Zugangsdaten - Newsletter (Zustimmung erforderlich)
Geschlecht	Geschlecht des Mitarbeiters	Geschlechtsspezifisches Wording
Position[1]	Position im Unternehmen	Betriebsinterne Kommunikation, Darstellung zur eindeutigen Rollenzuordnung
Telefonnummer[1]	Berufliche Telefonnummer des Mitarbeiters	Betriebsinterne Kommunikation
Geburtstag[1]	Geburtstag des Mitarbeiters	Betriebsinterne Kommunikation
Abteilung[1]	Abteilung, in der der Mitarbeiter tätig ist	Betriebsinterne Kommunikation, Darstellung zur eindeutigen Rollenzuordnung
Einstellungsdatum[1]	Datum Betriebseintritt	Betriebsinterne Kommunikation
Lichtbild[1]	Foto des Mitarbeiters oder Profilbild	Betriebsinterne Kommunikation, einfache Identifikation
Korrespondenzdaten, Daten zu Übersetzungen	Daten in Zusammenhang mit der Erbringung der geschuldeten	Betriebsinterne Kommunikation inkl des Google Übersetzers.

	Arbeitsleistung, Daten zu Gästeanfragen, Daten interner Chats und Vermerke sowie Daten in übersetzten Texten.[3]	
Textdaten, Inhaltsdaten	Von der betroffenen Person verfasste Inhalte, Kommentare, Korrespondenzen, Handbuchartikel.	betriebsinterne Kommunikation
Fotos und sonstige Dateien.	Von der betroffenen Person hochgeladene Fotos und sonstige Dateien.	betriebsinterne Kommunikation

Auftraggeberdaten

Bezeichnung	**Beschreibung**	**Verwendungszweck**
Name[2]	Vorname und Nachname des Betroffenen	Bereitstellung (Speicherung) der Kundeninformation
Kontaktinformation[2]	Hinterlegte Kontaktdaten, Adresse, E-Mail, Telefonnummer, Daten zum Unternehmen des Auftraggebers	Bereitstellung (Speicherung) der Kundeninformation

Lieferantendaten

Bezeichnung	**Beschreibung**	**Verwendungszweck**
Name[2]	Vorname und Nachname des Betroffenen	Bereitstellung (Speicherung) der Lieferanteninformation
Kontaktinformation[2]	Hinterlegte Kontaktdaten, Adresse, E-Mail, Telefonnummer, Unternehmenszugehörigkeit	Bereitstellung (Speicherung) der Lieferanteninformation

Kundendaten

Bezeichnung	**Beschreibung**	**Verwendungszweck**
Name[2]	Vorname und Nachname des Betroffenen	Bereitstellung (Speicherung) der Kundeninformation
Kontaktinformation[2]	Hinterlegte Kontaktdaten, Adresse, E-Mail, Telefonnummer	Bereitstellung (Speicherung) der Kundeninformation
Informationen zum Aufenthalt[2]	Angaben zur Dauer des Reiseaufenthaltes	Bereitstellung (Speicherung) der Kundeninformation
Nationalität[2]	Nationalität des Kunden	Bereitstellung (Speicherung) der Kundeninformation
Geschlecht[2]	Geschlecht des Kunden	Bereitstellung (Speicherung) der Kundeninformation
Informationen zu Anfragen und Vorfällen[2]	Korrespondenzdaten und Daten zu Anfragen sowie Vorfällen in Zusammenhang mit Kunden des Auftraggebers	Kommunikation und Bereitstellung (Speicherung) der Kundeninformation.
Daten zu Übersetzungen[3]	Alle mittels dem Google Übersetzer übersetzen Datenkategorien, insbesondere auch Daten zu Anfragen von Gästen oder Daten interner Vermerke sowie Daten in übersetzten Texten.[3]	Kommunikation inkl des Google Übersetzers und Bereitstellung (Speicherung) der Kundeninformation.
Fotos und Dateien[2]	Von den Mitarbeitern des Auftraggebers hochgeladene Fotos und Dateien.	Bereitstellung (Speicherung) der Kundeninformation

Fußnoten:

[1]optional, soweit durch den jeweiligen Nutzer hinterlegt
[2]optional, sofern diese Information durch den Auftraggeber in der Plattform gespeichert wird
[3]Darüber hinaus werden bei der Nutzung des Google Übersetzers Dienstdaten generiert (siehe die Datenschutzhinweise von Google).

Teil B: Technische Daten

Dieser Teil enthält Daten, die der Betroffene durch Aktivität innerhalb des Netzwerkes generiert. Sämtliche Daten werden hierbei durch die betroffene Person selbst erhoben.

Diese Daten betreffen sämtliche der oben genannten Kategorien betroffener Personen.

Bezeichnung	**Beschreibung**	**Verwendungszweck**
Aktivität	Bezeichnung der durchgeführten Aktivität	- Betriebsinterne Kommunikation - Nachvollziehbarkeit von Aktivitäten
Erstellungszeit	Zeitpunkt, zu der die Aktivität durchgeführt bzw. Inhalte erstellt wurden	- technisch notwendig - zur Nachvollziehbarkeit von Aktivitäten
Zeitpunkt Lesezugriff	Zeitpunkt, zu dem ein Mitarbeiter neue Inhalte erstmalig abgerufen hat	- technisch notwendig für Information über Änderungen - Nachvollziehbarkeit der Kenntnisnahme
IP-Adresse	IP-Adresse des Anschlusses, von dem aus der Zugriff erfolgt	Gewährleistung von Datensicherheit, technisch notwendig
Übertragene Daten	Menge der übertragenen Daten	Gewährleistung von Datensicherheit
Browser und Geräteversion	Verwendeter Browser und Geräte	Datensicherheit, Bereitstellung Funktionalitäten je nach Kompatibilität
Modell	Bei Nutzung von iOS- oder Android-App: Modellbezeichnung	Für die Bereitstellung von Funktionen je nach Kompatibilität mit dem Gerät
Letzter Login	Letztmaliger aktiver Login auf der Plattform	Gewährleistung von Datensicherheit

Zusätzliche technische Daten iZm App-Nutzung

Bezeichnung	**Beschreibung**	**Verwendungszweck**
Session-Gerätedaten	Gerätename, Gerätehersteller, Location, Session-Zeitpunkt	Sicherheitsfunktion: Anzeige angemeldeter Geräte

Anlage 2: Technische & organisatorische Maßnahmen

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.
Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Um physischen Zugriff auf die Daten des Auftraggebers zu verhindern, befindet sich dauerhaft Sicherheitspersonal in den Rechenzentren des Auftragnehmers. Diese sind zudem in allen Bereichen videoüberwacht.

2. Zugangskontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz), Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Zugriff auf die Server haben ausschließlich autorisierte Techniker mit den entsprechenden individuellen Benutzerrechten. Sichere Zugangsverbindungen (mittels verschlüsselten VPN-Tunnel) und Technologien zur Authentifizierungskontrolle (Authentifikation über Benutzername und Passwort) sind implementiert, um den Zugang zu den Systemen und zum internen Support zu reglementieren.

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.
Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Der Auftraggeber bestimmt über die Benutzereinstellungen und das Rechtemanagement in der Software, wer auf welche Informationen Zugriff hat.
- Der Auftraggeber legt Richtlinien zur Länge, Komplexität, und Ablauf von Passwörtern fest.
- Durch die vorgenannten Zugangskontrollen wird der Zugriff auf die im Rahmen der Services erfassten personenbezogenen Daten abgesichert.
- Der Zugriff ist zudem mittels eines Berechtigungskonzepts auf Mitarbeiter des Auftragnehmers mit entsprechenden Verantwortlichkeiten beschränkt.
- Die Anzahl der Mitarbeiter des Auftragnehmers mit Berechtigungen ist auf das „Notwendigste“ reduziert.

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle, …
Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Die Übertragung der Daten findet mittels https Protokoll statt. Durch den Einsatz aktueller Verschlüsselungen auf Basis TLS (Transport Layer Security) gewährleistet der Auftragnehmer den derzeit höchstmöglichen Schutz der Daten im Zuge der Übermittlung.

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.
Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Der Zugriff bzw. die Veränderung der übermittelten personenbezogenen Daten unterliegt wirksamen Zugriffsschutzmechanismen wie oben unter Ziffer 3 beschrieben. Eingaben, Veränderungen und Löschungen von Daten werden mittels Session-Logs protokolliert.

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.
Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Wenn der Auftraggeber die Weisung erteilt, dass personenbezogen Daten eingegeben, verändert oder entfernt werden sollen, ist aufgrund der Beschaffenheit der Software und des Systems gewährleistet, dass diese Weisungen jederzeit umgesetzt werden können.
- Die Auswahl der Subunternehmer wurde unter Sorgfaltsgesichtspunkten insbesondere hinsichtlich Datensicherheit vom Auftragnehmer getroffen.
- Die Kontrollrechte gegenüber dem Auftragnehmer wurden definiert.
- Die Mitarbeiter des Auftragnehmers wurden zum Datengeheimnis verpflichtet.
- Die Vernichtung der Daten nach Beendigung des Auftrages ist sichergestellt.

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.
Maßnahmen zur Datensicherung (physikalisch / logisch):

- Durch die Verteilung der Systeme auf verschiedene Rechenzentren kann eine sehr hohe Verfügbarkeit erreicht und Wartungsarbeiten an der Infrastruktur ohne Auswirkungen auf die Erreichbarkeit ausgeführt werden.
- Sämtliche Änderungen werden in stündlichen Backups erfasst. Wöchentliche Backups sorgen zudem für eine weitere Sicherheit gegen Datenverlust und ermöglichen ein stabiles und schnelles Wiederherstellen von Datenbanken und Dateien.
- Sämtliche eingesetzte Software wird regelmäßig auf den aktuellsten Stand gebracht. Somit werden mögliche Sicherheitslücken in allen Bereichen schnellstmöglich behoben.
- Der Einsatz von Antiviren-Programmen und einer Firewall verhindert das Auftreten von Schadcode.
- Die Überwachung aller Ressourcen ermöglicht ein präventives Eingreifen und dient der Früherkennung von Problemen und möglichen Angriffen. So kann sichergestellt werden, dass ein reibungsloser und sicherer Zugriff möglich ist.
- Die ausgewählten Rechenzentren verfügen über eine exzellente Anbindung an das Internet. Durch die direkte Anbindung der in der Anlage genannten Subauftragnehmer ist ein schneller und stabiler Zugriff weltweit ermöglicht. Auch hier kann mit verschiedenen Routen eine hohe Verfügbarkeit auch bei Störungen außerhalb des Rechenzentrums gewährleistet werden.

- Meldewege sind definiert und den Mitarbeitern bekannt
- Notfallpläne zur schnellen Wiederherstellung sind vorhanden und werden regelmäßig auf ihre Wirksamkeit hin überprüft

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.
Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Die Verarbeitung, sowie Backups werden grundsätzlich auf mehreren Speichermedien in räumlich getrennten Bereichen aufbewahrt, um eine Trennung zu gewährleisten.
- Die Datensätze werden mit Zweckattributen versehen.
- Es sind eindeutige Datenbankrechte festgelegt.
- Es ist eine logische softwareseitige Mandantentrennung gegeben.
- Eigene Entwicklungs-, Test- und Produktivsysteme gewährleisten eine eindeutige Trennung der verwendeten Daten.

9. Pseudonymisierung

Verarbeitung von Daten in einer Weise, die keine Zuordnung von Daten zu spezifischen Personen ohne das Hinzuziehen zusätzlicher Informationen aus getrennter Quelle ermöglicht:

- Pseudonymisierung durch Verwendung von eindeutigen Identifikationsnummern (ID)
- Getrennte Speicherung der Zuordnung von ID zu spezifischen Personen

10. Weitere Maßnahmen

Um den besonderen Anforderungen des Datenschutzes gerecht zu werden, wurden zudem Anpassungen und innerbetriebliche Maßnahmen getroffen:

- Erarbeitung eines Datenschutz- und IT-Sicherheitskonzeptes
- Regelmäßige Schulungen für Mitarbeiter
- Einführung eines Datenschutz-Managementsystems mit Prozessen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von getroffenen Maßnahmen
- datenschutzfreundliche Voreinstellungen

Anlage 3: Sub-Auftragsverarbeiter

Subauftragsverarbeiter Infrastruktur – Datenspeicherung			
Name des Unternehmens	Anschrift	Übernommene Dienstleistung	Maßnahmen angemessenen Datenschutzniveaus
hotelkit technik UG	hotelkit technik UG (haftungsbeschr.), Teplitzer Str. 34, D-01219 Dresden	• Entwicklung der Plattform • Betreuung der Server- und Netzwerkinfrastruktur der hotelkit GmbH	Auftragsverarbeitervertrag
1&1 IONOS SE	1&1 IONOS SE, Elgendorfer Str. 57, D-56410 Montabaur	• Bereitstellung Virtual Server für Live-Umgebung • Datenstandort: Karlsruhe	Auftragsverarbeitervertrag
diva-e NEXT GmbH	diva-e Datacenters GmbH, Kruppstraße 105, D-60388 Frankfurt/Main	• Bereitstellung Dedicated Server für Live-Umgebung • Datenstandort: Frankfurt	Auftragsverarbeitervertrag
ANEXIA Internetdienstleistungs GmbH	Anexia Deutschland GmbH, Hofmühlgasse 3, A-1060 Wien	• Bereitstellung Virtual Server für Reverse Proxy Server • Datenstandort: Wien	Auftragsverarbeitervertrag
Hetzner Online GmbH	Hetzner Online GmbH, Industriestr. 25, D-91710 Gunzenhausen	• Bereitstellung Dedicated Server für Ablage verschlüsselter Backups • Datenstandort: Falkenstein in Sachsen	Auftragsverarbeitervertrag

Subauftragsverarbeiter Servicespezifisch			

Name des Unternehmens	Anschrift	Übernommene Dienstleistung	Maßnahmen angemessenen Datenschutzniveaus
Microsoft Corporation	Walter-Gropius-Straße 5, 80807, München, Deutschland	• Verwaltung SMTP-Relay	Auftragsverarbeitervertrag Für dieses Drittland liegt ein Angemessenheitsbeschluss der EU-Kommission vor, den Sie hier abrufen können. Die Microsoft Corporation ist unter dem Angemessenheitsbeschluss der EU-Kommission zugrundeliegenden EU-U.S.-Data Privacy Framework zertifiziert. Die Zertifizierung können Sie hier abfragen.
salesforce.com Germany GmbH	Erika-Mann-Str. 31, 80636, München, Deutschland	• CRM und Leadmanagement	Auftragsverarbeitervertrag
Atlassian, Public limited company	Level 6, 341 George Street, NSW 2000, Sydney, Australien	• Verwaltung und Weiterleitung von Support-Anfragen	Auftragsverarbeitervertrag und Standardvertragsklauseln für die Übermittlung in Drittländer
Google Cloud EMEA Limited* * für Nutzer in Österreich. Die in anderen Ländern zuständige Google-Gesellschaft kann unter folgendem Link abgefragt werden: https://cloud.google.com/terms/google-entity.	70 Sir John Rogerson's Quay, Dublin 2, Irland	• Automatische Übersetzung von durch den Autor eingegebenen Texten (Nutzung mehrerer Sprachen) mittels dem Google Übersetzer	Auftragsverarbeitervertrag
Celonis SE	Theresienstr. 6, 80333, München, Deutschland	• CRM und Leadmanagement • Automation	Auftragsverarbeitervertrag

PandaDoc, Inc.	3739 Balboa Street. Suite #1083, San Francisco, CA 94121, USA	• Angebots- und Vertragserstellung und Verwaltung • Erstellen von E-Signaturen	Auftragsverarbeitervertrag Für dieses Drittland liegt ein Angemessenheitsbeschluss der EU-Kommission vor, den Sie hier abrufen können. Die PandaDoc, Inc. ist unter dem Angemessenheitsbeschluss der EU-Kommission zugrundeliegenden EU-U.S.-Data Privacy Framework zertifiziert. Die Zertifizierung können Sie hier abfragen.
HubSpot, Inc.	25 First Street, Cambridge, MA 02141 USA	• CRM and Marketing Management	Auftragsverarbeitervertrag Für dieses Drittland liegt ein Angemessenheitsbeschluss der EU-Kommission vor, den Sie hier abrufen können. Die HubSpot, Inc. ist unter dem Angemessenheitsbeschluss der EU-Kommission zugrundeliegenden EU-U.S.-Data Privacy Framework zertifiziert. Die Zertifizierung können Sie hier abfragen.