MASCH Software Solutions
Paulinenweg 3 - 51149 Köln, Deutschland

Vertrag zur Auftragsverarbeitung für CLOUD Services
zwischen
Musterhotel

Musterstr. 10

51149 Musterstadt

vertreten durch Robert Mustermann, Inhaber

im Folgenden Auftraggeber genannt und der

MASCH Customer Service Group
repräsentiert durch Schaarschmidt Hard- & Software e.K.
Paulinenweg 3 – 51149 Köln
vertreten durch Martin Schaarschmidt, Inhaber & Geschäftsführer

im Folgenden Auftragsverarbeiter genannt,

schließen folgenden Vertrag:

§1 Allgemeine Bestimmungen und Auftragsgegenstand

1. Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Verarbeitung sind Anlage 1 zu entnehmen.
2. Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für die Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.
3. Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.
4. Die Vergütung wird außerhalb dieses Vertrags vereinbart.
5. Der Auftragsverarbeiter bedient sich des Rechenzentrums der

   PLUTEX GmbH
   Vertreten durch Torben Belz, Geschäftsführer
   Hermann-Ritter-Straße 108 - 28197 Bremen

   als Subunternehmer, mit dem der Auftragsverarbeiter einen gleichlautenden Vertrag als Subunternehmer des Auftragsverarbeiters abgeschlossen hat.

§2 Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

§3 Weisungen des Auftraggebers

1. Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.
2. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.
3. Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.
4. Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

§4 Kontrollbefugnisse des Auftraggebers

1. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.
2. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.
3. Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

§5 Allgemeine Pflichten des Auftragsverarbeiters

1. Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen zu implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.
3. Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.
4. Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.
5. Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.
6. Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

§6 Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.
2. Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

§7 Unterstützungspflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 - 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.
2. Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 - 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

§8 Einsatz von Unterauftragsverarbeitern (Subunternehmer)

1. Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmer-verhältnisse des Auftragsverarbeiters sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 2 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.
2. Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und Integrität der Hard-und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.
3. Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.
4. Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur

Ausübung der gleichen Kontrollrechte, wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.

5. Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.
6. Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.
7. Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese - soweit gesetzlich vorgeschrieben - einen Datenschutzbeauftragten benannt haben.
8. Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

§9 Mitteilungspflichten des Auftragsverarbeiters

1. Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.
2. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.
3. Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.
4. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

§10 Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

MASCH Software Solutions
Paulinenweg 3 - 51149 Köln, Deutschland

§11 Datengeheimnis und Vertraulichkeit

1. Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.
2. Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutz-bestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.
3. Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

§12 Schlussbestimmungen

1. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.
2. Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.
3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.
4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.
5. Es werden neben den hier vereinbarten Bestimmungen die gesetzlichen Datenschutz-bestimmungen der Bundesrepublik Deutschland und der Europäischen Union durch den Auftragsverarbeiter anerkannt.

Martin Schaarschmidt	Robert Mustermann
Leiter MASCH Customer Service Group	Inhaber
Inhaber Schaarschmidt Hard- & Software e.K.	Musterhotel

DIESER VERTRAG BEDARF KEINER UNTERSCHRIFT, DA BEIDE PARTNER DIESEM VERTRAG DURCH DIGITALE PRÜFUNG ZUGESTIMMT HABEN.

MASCH Software Solutions
Paulinenweg 3 - 51149 Köln, Deutschland

Anlage 1 - Auftragsdetails

Der vorliegende Vertrag umfasst (im Zusammenhang mit dem Rahmenvertrag und der Leistungsbeschreibung) zusammengefasst die folgenden Leistungen.

1. Speicherkapazität für kundeneigene Daten auf Servern und Cloud-Laufwerken von Server-Systemen und dort betrieben Anwendungen (Datenbank-, Backup-, Web-Server, SAN-Umgebung)
2. technische Administration der Server-Systeme
3. Support-Tätigkeiten für sämtliche Server-Systeme
4. Betreuung, der von der Auftraggeberin betriebenen Firewall (Log-Files)

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

1. Stammdaten
2. Kontaktdaten
3. Vertragsdaten
4. Vertragssteuerungsdaten
5. Protokolldaten
6. Daten und Inhalte der CLOUD Anwendung

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

1. Kunden und potentielle Kunden des Auftraggebers (Endverbraucher)
2. Beschäftigte, Lieferanten und Geschäftspartner des Auftraggebers

Umfang, Art und Zweck der Zugriffsmöglichkeit des Auftragsverarbeiters auf Daten des Auftraggebers ergeben sich aus den Leistungsbeschreibungen der CLOUD-Anwendung CM Studio .VIG-CLOUD und den damit verbundenen Hosting-Leistungen.

MASCH Software Solutions
Paulinenweg 3 - 51149 Köln, Deutschland

Anlage 2 - Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters (Schaarschmidt Hard- & Software e.K.) nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

Zweckbindung und Trennbarkeit

Folgende Maßnahmen des Auftragsverarbeiters gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

1. Logische Mandantentrennung (softwareseitig)
2. Berechtigungskonzept (siehe Anlage 5)
3. Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
4. Trennung von Produktiv- und Testsystem
5. Logfiles - In den Server-Log-Dateien werden Informationen gespeichert, die Ihre Anwendung zum Teil automatisch an uns übermittelt oder die bei der Bearbeitung Ihrer Anfrage entstehen. Dies sind: Aufgerufene Anwendung/ Web-Seite, Browsertyp/ Browserversion, verwendetes Betriebssystem, Referrer URL, IP-Adresse des zugreifenden Rechners, Uhrzeit der Serveranfrage. Damit diese Daten nicht bestimmten Personen oder Absendern zu zu ordnen sind, wird bei der Speicherung das letzte Oktett der IP-Adresse entfernt. Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen.

Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme Auftragsverarbeiters:

1. Verschlüsselung - Datenübertragungen werden per TLS verschlüsselt (bspw. HTTPS oder SSH). VPN-Zugänge erfolgen über persönliche Accounts mit IPSec.
2. Pseudonymisierung - „Pseudonymisierung" bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt.
3. Zutrittskontrolle - Es wurden folgende Maßnahmen durch den Auftragsverarbeiter für seine Büroräumlichkeiten getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:
    a. Dreifache Schliessanlage am Eingang
    b. Fenster einbruchsicher abgesichert
4. Zugangskontrolle - Es wurden folgende Maßnahmen durch den Auftragsverarbeiter getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:
    a. Festlegung und Review von Benutzerrechten
    b. Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
    c. Zuordnung von Benutzerprofilen zu IT-Systemen
    d. Einsatz von VPN-Technologie bei der Übertragung von Daten
    e. Verschlüsselung mobiler IT-Systeme
    f. Verschlüsselung mobiler Datenträger

g. Verschlüsselung der Datensicherungssysteme
h. Sperren externer Schnittstellen (USB etc.)
i. Einsatz von Intrusion-Detection-Systemen
j. Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
k. Einsatz von Anti-Viren-Software
l. Verschlüsselung von Datenträgern in Laptops / Notebooks
m. Einsatz einer redundanten Hardware-Firewall

5. Zugriffskontrolle - Es wurden folgende Maßnahmen durch den Auftragsverarbeiter getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
   a. Berechtigungskonzept
   b. Verwaltung der Rechte durch Systemadministrator
   c. regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
   d. Anzahl der Administratoren auf das „Notwendigste“ reduziert
   e. Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
   f. Sichere Aufbewahrung von Datenträgern
   g. physische Löschung von Datenträgern vor Wiederverwendung
   h. ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
   i. Protokollierung der Vernichtung
6. Eingabekontrolle - Mit Hilfe folgender Maßnahmen kann nachträglich durch den Auftragsverarbeiter überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
   a. Protokollierung der Eingabe, Änderung und Löschung von Daten
   b. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
   c. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
7. Auftragskontrolle - Folgende Maßnahmen des Auftragsverarbeiters gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
   a. schriftliche Weisungen an den Auftragsverarbeiter
   b. Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
   c. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
8. Transport- bzw. Weitergabekontrolle - Folgende Maßnahmen des Auftragsverarbeiters gewährleisten, dass personen- bezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:
   a. Einsatz von VPN-Tunneln
   b. Verschlüsselung der Daten über 2-Wege Verfahren (Public/Private Key)
9. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen – Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von einem Jahr durch einen externen Prüfer und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen und falls notwendig Änderungen und Anpassungen dem Auftragsverarbeiter mitteilen.

MASCH Software Solutions
Paulinenweg 3 - 51149 Köln, Deutschland

Anlage 3 - Liste der bestehenden technischen und organisatorischen Maßnahmen der Plutex GmbH als Subunternehmer des Auftragsverarbeiters nach Art. 32 DSGVO

Plutex GmbH setzt im Auftrag des Auftragsverarbeiters folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

Zweckbindung und Trennbarkeit

Folgende Maßnahmen der Plutex GmbH gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

1. physikalisch getrennte Speicherung in verschiedenen Brandabschnitten, auf gesonderten Systemen oder Datenträgern
2. Logische Mandantentrennung (softwareseitig)
3. Berechtigungskonzept
4. Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
5. Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
6. Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
7. Trennung von Produktiv- und Testsystem
8. Logfiles - In den Server-Log-Dateien werden Informationen gespeichert, die Ihre Anwendung zum Teil automatisch an uns übermittelt oder die bei der Bearbeitung Ihrer Anfrage entstehen. Dies sind: Aufgerufene Anwendung/ Web-Seite, Browsertyp/ Browserversion, verwendetes Betriebssystem, Referrer URL, IP-Adresse des zugreifenden Rechners, Uhrzeit der Server-anfrage. Damit diese Daten nicht bestimmten Personen oder Absendern zu zu ordnen sind, wird bei der Speicherung das letzte Oktett der IP-Adresse entfernt. Alle nutzungsspezifischen Einträge in den Server-Log-Dateien werden nach 7 Tagen automatisch entfernt. Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen.

Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme der Plutex GmbH im Auftrag des Auftragsverarbeiters:

1. Verschlüsselung - Datenübertragungen werden per TLS verschlüsselt (bspw. HTTPS oder SSH). VPN-Zugänge erfolgen über persönliche Accounts mit IPSec.
2. Pseudonymisierung - „Pseudonymisierung" bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt. Plutex GmbH pseudonymisiert Kundendaten des Auftragsverarbeiters im Rahmen der Entwicklung des eigenen ERP-Systems PONG. Eine weitere Pseudonymisierung von Daten findet nicht statt.
3. Zutrittskontrolle - Es wurden folgende Maßnahmen durch die Plutex GmbH getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:
    a. Alarmanlage

   b. Chipkarten-/Transponder-Schließsystem mit Pin-Code (2-Faktor-Authentisierung)
   c. Videoüberwachung der Zugänge
   d. Personenkontrolle beim Pförtner / Empfang
   e. Protokollierung der Besucher
   f. Tragepflicht von Berechtigungsausweisen
4. Zugangskontrolle - Es wurden folgende Maßnahmen durch die Plutex GmbH getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:
   a. Festlegung und Review von Benutzerrechten
   b. Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
   c. Zuordnung von Benutzerprofilen zu IT-Systemen
   d. Einsatz von VPN-Technologie bei der Übertragung von Daten
   e. Verschlüsselung mobiler IT-Systeme
   f. Verschlüsselung mobiler Datenträger
   g. Verschlüsselung der Datensicherungssysteme
   h. Sperren externer Schnittstellen (USB etc.)
   i. Einsatz von Intrusion-Detection-Systemen
   j. Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
   k. Einsatz von Anti-Viren-Software
   l. Verschlüsselung von Datenträgern in Laptops / Notebooks
   m. Einsatz einer redundanten Hardware-Firewall
5. Zugriffskontrolle - Es wurden folgende Maßnahmen durch die Plutex GmbH getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
   a. Berechtigungskonzept
   b. Verwaltung der Rechte durch Systemadministrator
   c. regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
   d. Anzahl der Administratoren auf das „Notwendigste“ reduziert
   e. Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
   f. Sichere Aufbewahrung von Datenträgern
   g. physische Löschung von Datenträgern vor Wiederverwendung
   h. ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
   i. Einsatz von Aktenvernichtungs-Dienstleistern (zertifiziert)
   j. Protokollierung der Vernichtung
6. Eingabekontrolle - Mit Hilfe folgender Maßnahmen kann nachträglich durch die Plutex GmbH überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
   a. Protokollierung der Eingabe, Änderung und Löschung von Daten
   b. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
   c. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
7. Auftragskontrolle - Folgende Maßnahmen der Plutex GmbH gewährleisten, dass personenbezogene

Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
   a. schriftliche Weisungen an den Auftragsverarbeiter
   b. Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
   c. Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
   d. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
   e. Vertragsstrafen bei Verstößen
8. Transport- bzw. Weitergabekontrolle - Folgende Maßnahmen der Plutex GmbH gewährleisten, dass personen- bezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:
   a. Einsatz von VPN-Tunneln
   b. Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E- Mail-Verkehrs)
   c. Verschlüsselung physischer Datenträger bei Transport
9. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme - Folgende Maßnahmen der Plutex GmbH gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
   a. Unterbrechungsfreie Stromversorgung (USV)
   b. Klimatisierung der Serverräume
   c. Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
   d. Feuer- und Rauchmeldeanlagen in Serverräumen
   e. Feuerlöschgeräte in Serverräumen
   f. Alarmmeldung bei unberechtigten Zutritten zu Serverräumen oder nicht ordnungsgemäß geschlossenen Türen
   g. Erstellen, Pflege und Test eines Backup- und Recoverykonzepts
   h. Erstellen eines Notfallplans
   i. Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
   j. Serverräume über der Wassergrenze
10. Besondere Datenschutzmaßnahmen der Plutex GmbH liegen bei der Plutex GmbH schriftlich vor:
   a. interne Verhaltensregeln
   b. Risikoanalyse
   c. Datensicherheitskonzept
   d. Wiederanlaufkonzept
   e. Zertifikat ISO 27001, Zertifikat ISO 9001
11. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen – Die Plutex GmbH wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von einem Jahr durch einen externen Prüfer und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen und falls notwendig Änderungen und Anpassungen dem Auftragsverarbeiter mitteilen.

MASCH Software Solutions
Paulinenweg 3 - 51149 Köln, Deutschland

Anlage 4 - Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

1. PLUTEX GmbH, vertreten durch Torben Belz, Geschäftsführer, Hermann-Ritter-Straße 108 28197 Bremen

MASCH Software Solutions
Paulinenweg 3 - 51149 Köln, Deutschland

Anlage 5 – Beschreibung der Zugriffssicherungen auf den Datenbestand in der CLOUD-Anwendung

1. Der Auftragsverarbeiter hat gemäß dem Zugriffsberechtigungsverfahren der Software Anwendung CM Studio .V.I.G.-CLOUD nur einen stark limitierten Zugriff auf die personenbezogenen Daten in der Anwendung.
2. Der Zugriff auf personenbezogene Daten ist für den Support des Auftragsverarbeiters nur bei expliziter Datenfreigabe durch den um Support anfragenden Betrieb gewährleistet. Derartige Datenfreigabe wird im Systemprotokoll der Anwendung protokolliert und dokumentiert.

Das Zugriffsberechtigungsverfahren der Software CM Studio .V.I.G.-CLOUD sieht folgende Funktionalität vor:

Zugriffsberechtigungskonzept von CM Studio .V.I.G.-CLOUD

Da die Anzahl der Benutzer im System sehr groß sein kann, werden für die Definition der Zugriffsberechtigungen sogenannte Rollen (oder auch als Gruppen bezeichnet) verwendet, die dann an einzelne Benutzer vergeben werden können.

Vordefinierte Benutzer

admin

Der ‚admin' ist ein vordefinierter Master-Administrator, der sich auch ohne Datenbank-Verbindung einloggen kann und zum Beispiel die Datenbank-Verbindung anpassen kann. In normalen administrativen Bereichen der CM Studio Anwendung hat dieser Benutzer absoluten Zugriff.

Im Programmbereich der CM Studio .V.I.G.-CLOUD ist dieser Benutzer komplett gesperrt.

ccadmin

Der ‚ccadmin' ist ein spezieller Benutzer für das Zugriffs- und Berechtigungs-Management von Kreditkartenzugängen verwendet wird. Der ‚ccadmin' ist dabei einzig in der Lage anderen Benutzern den Kreditkartenzugang zu vergeben. Diese Benutzer werden dann automatisch mit der Zugriffsrolle ‚Credit Card Access' versehen. Im Modul- und Programmbereich der V.I.G.- CLOUD ist dieser Benutzer komplett gesperrt und wird nicht verwendet.

supportadmin

Der ‚supportadmin' ist ein spezieller Benutzer, der automatsch angelegt wird, und zu Supportzwecken durch den IT- und Anwendungssupport des Lizenznehmers der CM Studio Anwendung verwendet werden kann. In den normalen Bereichen der CM Studio Anwendung hat dieser Benutzer absoluten Zugriff. Gegenüber dem ‚admin' Account verfügt er über einige wenige Restriktionen im Zugriff auf die Datenbankverbindung. Der ‚supportadmin' benötigt eine valide Datenbank-Verbindung um sich in die CM Studio Anwendung einzuloggen. Für den Zugriff auf personenbezogene Daten im Modul- und Programmbereich der V.I.G.-CLOUD ist dieser Benutzer per Default gesperrt. Falls ein Anwender entsprechenden Support benötigt, kann er dem

‚supportadmin' die Berechtigung geben auf die geschützten Daten- und Programmbereiche zuzugreifen. Nach erfolgter Supporttätigkeit muss der Anwender dann die Berechtigungsfreigabe wieder deaktivieren. Alle Tätigkeiten und Aktionen, die der ‚supportadmin' im Rahmen der Anwenderfreigabe tätigt, werden in einem separaten Protokoll protokoliert und festgehalten.

Vordefinierte Gruppen

Administratoren

Die sogenannten Systemadministratoren haben innerhalb von der CM Studio Anwendung auf alle ‚normalen Bereiche' wie Website-Content etc. Zugriff und die Berechtigung diese zu pflegen. Hierfür können Sie im Einzelfall auch Website-**Operatoren** einrichten.

‚Administratoren' ist hierbei eine Gruppe, die einem personalisierten Service-Mitarbeiter des Lizenznehmers als Rolle zugewiesen werden kann.

GRM Administratoren (nur bei CM Studio .V.I.G.-CLOUD verwendbar)

Die Benutzer mit dieser Rolle sind Hoteliers bzw. Hotel-Manager, die über Administrationsrechte innerhalb des Mandanten-Accounts Ihres Hotels verfügen. Das System stellt diesen Anwendern eine eigene virtuelle Umgebung im System zur Verfügung, in der Sie die Funktionen des digitalen Meldewesens definieren und organisieren können.

GRM Operatoren (nur bei CM Studio .V.I.G.-CLOUD verwendbar)

Die Anwender, die über diese Rolle verfügen, sind immer einem spezifischen GRM Administrator zugeordnet und dürfen die Gästedaten des Hotels bearbeiten. Sie können aber nicht die Grundeinstellungen des Mandanten-Accounts einsehen oder verändern. So kann der Hotelier eigenen Mitarbeitern Zugriff auf die Gästeverwaltung gewähren, Ihnen aber keine Veränderungen am Setup erlauben.

GRM Tourist Admin (nur bei CM Studio .V.I.G.-CLOUD verwendbar)

Die Anwender mit dieser Rolle verfügen über Administrationsrechte innerhalb des Destinations-Interfaces von CM Studio .V.I.G.-CLOUD. Hierbei ist zu vermerken, dass Daten, die noch nicht reportet wurden durch das Hotel, auch nicht vom ‚GRM Tourist Admin' eingesehen werden können. Einen Zugriff auf die Daten hat dieser Anwender erst, wenn die Daten durch das Hotel an die Destination reportet wurden. Der ‚GRM Tourist Admin' ist hierbei berechtigt weitere Mitarbeiter einzurichten, die als , GRM Tourist Operator' die Auswertung der Daten und die Übergabe der Daten an das externe Finanzsystem bearbeiten. Der ‚GRM Tourist Admin' hat Zugriff auf die personenbezogenen Daten ab dem Zeitpunkt, wo das Hotel Daten in das Meldearchiv der Destination reportet hat. Er kann ähnlich wie der ‚supportadmin' auf Anfrage des Hotels auch Supportleistungen im Hotel-Interface erbringen, wenn das Hotel ihm temporär Zugriff auf die Daten gibt.

GRM Tourist Operator (nur bei CM Studio .V.I.G.-CLOUD verwendbar)

Der ‚GRM Tourist Operator' ist für die Auswertung der Daten und die Übergabe der anonymisierten Reporting-

Daten an das externe Finanzsystem verantwortlich. Er hat keinen Zugriff auf die personenbezogenen Daten.

GRM Police (nur bei CM Studio .V.I.G.-CLOUD verwendbar)

Die Benutzer mit dieser Rolle dürfen auf alle personenbezogenen Daten im Modul- und Programmbereich der GRM-CLOUD zugreifen. Dies gilt sowohl für die aktiven Daten im Hotel-Interface als auch das Meldearchiv im Destinations-Interface. Um eine erhöhte Sicherheit für den Zugriff solcher Anwender zu gewährleisten, kann der Zugriff dieser Anwender auf bestimmte IPs begrenzt werden.

V.I.G.-CLOUD Administratoren (nur bei CM Studio .V.I.G.-CLOUD verwendbar)

Die Benutzer mit dieser Rolle sind Hoteliers bzw. Hotel-Manager, die über Administrationsrechte innerhalb des Mandanten-Accounts Ihres Hotels verfügen. Das System stellt diesen Anwendern eine eigene virtuelle Umgebung im System zur Verfügung, in der Sie die Funktionen der V.I.G.-CLOUD definieren und organisieren können.