

Vereinbarung zur Datenverarbeitung im Auftrag

1. Präambel

1.1 Die Straiv GmbH, Industriestraße 23, 70565 Stuttgart (nachfolgend „**Auftragsverarbeiter**“) stellt dem Kunden (nachfolgend „**Auftraggeber**“) die in der Individualvereinbarung bzw. den ergänzend einbezogenen Allgemeinen Geschäftsbedingungen und produktspezifischen Vertragsbedingungen (nachfolgend zusammengefasst **Hauptvertrag**) vereinbarten Leistungen (nachfolgend **Software**) bereit.

1.2 Der **Gegenstand des Auftrags** ist die Bereitstellung von Software in einem Rechenzentrum zum Zugriff und zur Nutzung über das Internet als Software-as-a-Service-Lösung sowie die Ermöglichung der Speicherung von Daten durch den Auftraggeber auf Servern, die im Auftrag des Auftragsverarbeiters betrieben werden. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 28 DSGVO auf Grundlage dieses Vertrages.

1.3 Die vertraglich **vereinbarte Leistungserbringung** wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

1.4 Die **Dauer dieses Auftrags** (Laufzeit) entspricht der Laufzeit des Hauptvertrages. Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

2. Zweck, Umfang und Art der Verarbeitung, Kategorien betroffener Personen sowie Art der personenbezogenen Daten

2.1 Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden. **Zweck, Umfang und Art der Verarbeitung** ergeben sich aus dem Hauptvertrag. Die Erhebung und/oder Verarbeitung und/oder Nutzung der Daten des

Auftraggebers dient der Erfüllung der Leistungen des Auftragnehmers im Sinne des Hauptvertrages.

2.2 Die **Kategorien betroffener Personen**, deren personenbezogene Daten übermittelt werden.

- Nutzer bzw. Beschäftigte/Angestellte des Auftraggebers (“Hotelpersonal”)
- Endnutzer bzw. Kunden des Auftraggebers (“Hotelgäste”)

2.3 Die **Art der personenbezogenen Daten**, die abhängig vom gewählten Softwarepaket und individuellen Einstellungen des Auftraggebers, übermittelt werden

- Nutzer bzw. Beschäftigte/Angestellte des Auftraggebers (“Hotelpersonal”)
 - Stamm- und Kommunikationsdaten (z.B. Vor-/Nachname, E-Mail-Adresse, Telefonnummer)
 - Nutzungsdaten (z.B. Dauer der Nutzung, genutztes Feature)
 - Bilddaten (optionales Profilbild)
- Endnutzer bzw. Kunden des Auftraggebers (“Hotelgäste”)
 - Stamm- und Kommunikationsdaten (z.B. Vor- und Nachname, E-Mail-Adresse, Telefonnummer)
 - Adressdaten (z.B. Straße, Hausnummer, PLZ, Stadt, Land)
 - Buchungs- bzw. Reisedaten (z.B. Anreise- und Abreisedatum, Buchungsnummer, Zimmernummer)
 - Meldescheindaten (z.B. Staatsangehörigkeit, Geburtsdatum, Passnummer, digitale Unterschrift)
 - Rechnungsdaten (z.B. Rechnungsadresse, Preise, gebuchte Services (z.B. Parken, Fitnessstudio))
 - Nutzungsdaten (z.B. Beginn, Dauer und Ende der Nutzung, genutztes Feature, genutzte Sprache, benutzter Browser und Betriebssystem)
 - Geodaten (nur bei Verwendung der Funktionalität “GPS-Einstellungen”, um die Services von Straiv auf einen Radius rund um das Hotel einzuschränken)

3. Pflichten und Weisungsbefugnisse des Auftraggebers

3.1 Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle Anfragen, sofern sie erkennbar ausschließlich an den

Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

3.2 Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Auftraggebers nur auf dessen dokumentierte Weisung. Der Auftraggeber erteilt alle Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem elektronischen Format zu bestätigen und zu dokumentieren.

3.3 Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung feststellt.

4. Pflichten des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

4.2 Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen als die in diesem Vertrag genannten sowie sich aus dem Hauptvertrag (siehe Ziff. 2.1) ergebenden Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer ist berechtigt, die im Auftrag verarbeiteten Daten zu anonymisieren und für eigene Zwecke, z.B. Produktanalyse, zu verwenden.

4.3 Der Auftragsverarbeiter wird im Rahmen der Verarbeitungstätigkeit alle hier vereinbarten Maßnahmen einhalten. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von

Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgenabschätzungen des Auftraggebers hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

4.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

4.5 Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Der Auftragsverarbeiter wird, soweit hier nicht anders vereinbart, keine aus dem Bereich des Auftraggebers erlangten Informationen an Dritte weitergeben.

4.6 Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Auftraggeber – in der Regel nach Terminvereinbarung – berechnigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der beauftragte Dritte darf nicht in einem unmittelbaren Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen. Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

4.7 Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO).

4.8 Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Beim Auftragsverarbeiter ist als externer Beauftragte(r) für den

Datenschutz bestellt: IITR Datenschutz GmbH, Marienplatz 2, 80331 München (Telefon: +49 89 189 173 60; E-Mail: email@iitr.de).

5. Mitteilungspflichten des Auftragsverarbeiters

Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters 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 Auftragsverarbeiter 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 Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

6. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftraggeber erteilt die allgemeine Genehmigung für die Beauftragung von Unterauftragnehmern. Insbesondere ist der Auftraggeber mit der Beauftragung der in **Anlage 2** aufgeführten Unterauftragnehmer einverstanden.

6.3 Der Einsatz weiterer Unterauftragnehmer oder der Wechsel der bestehenden

Unterauftragnehmer sind zulässig, soweit:

- der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab, mindestens jedoch 14 Tage vor dem geplanten Einsatz schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform innerhalb von 14 Tagen Einspruch mit sachlicher Begründung gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung mit dem Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

6.4 Erhebt der Auftraggeber aus sachlichem Grund gegen die Verarbeitung personenbezogener Daten durch den neuen Unterauftragnehmer Einspruch, ist jeder Vertragspartner berechtigt, den Hauptvertrag ohne Einhaltung einer Kündigungsfrist zu kündigen, insbesondere wenn ihm die Fortsetzung des Vertragsverhältnisses bis zur vereinbarten Beendigung oder bis zum Ablauf einer ordentlichen Kündigungsfrist nicht zumutbar ist.

6.5 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

7. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

7.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene und nachvollziehbare Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen berücksichtigt.

7.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet,

alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen.

7.3 Die aktuellen Maßnahmen können Anlage 1 entnommen werden und werden Bestandteil dieser Auftragsverarbeitung.

8. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber nach dessen Wahl auszuhändigen oder datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung wird dem Auftraggeber nach Aufforderung vorgelegt.

9. Haftung

9.1 Die Haftung richtet sich nach den gesetzlichen Bestimmungen gemäß Art. 82 DSGVO.

9.2 Die Parteien stellen sich jeweils von der Haftung für Schäden frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

10. Schlussbestimmungen

10.1 Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden

Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das für den Auftragsverarbeiter örtlich zuständige Gericht vereinbart.

10.2 Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich zu verständigen. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

10.3 Für die Auslegung dieser Vereinbarung ist die Version in der deutschen Sprache maßgeblich.

11. Salvatorische Klausel

Sollten eine oder mehrere Klauseln dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein, so soll dies die Gültigkeit der Vereinbarung im Übrigen nicht berühren. Die Parteien werden die unwirksame bzw. undurchführbare Klausel durch eine Bestimmung ersetzen, die dem Sinn und Zweck der unwirksamen Klausel zulässigerweise wirtschaftlich und rechtlich möglichst nahekommt. Das Gleiche gilt für Lücken in dieser Vereinbarung.

Anlage 1 - Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DSGVO und ggf. weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DSGVO. Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Zutrittskontrollsystem/Zutritt nur für autorisierte Mitarbeiter mittels Transponder-Schlüssel
- Zutrittskontrolle an der Haupteingangstüre mittels Kamera
- Dokumentierte Schlüsselvergabe
- Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung
- Empfang

1.2 Zugangskontrolle

- Kennwortrichtlinie (Mindestlänge, Alphanumerisch mit Groß- und Kleinschreibung sowie Sonderzeichen erforderlich)
- Der Login auf Serversysteme ist ausschließlich über SSH möglich, wobei nur Administratoren mit gültigen, über eine Whitelist mit RSA-SHA-Schlüsseln autorisierten Zugriffen und sicheren Passwörtern zugelassen werden.)
- Sperrung des Computers beim (temp.) Verlassen des Arbeitsplatzes
- Zugriff auf relevante System via OAuth und 2-Faktor Authentifizierung
- Firewall/Virenschanner
- Organisationsanweisung zur Ausgabe von Schlüsseln
- Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern (Richtlinie/Arbeitsanweisung)
- Gesicherte Übertragung von Authentifizierungsgeheimnissen (Credentials) mittels HTTPS

1.3 Zugriffskontrolle

- Differenzierte Berechtigungen (z.B. in Form von Profilen, Rollen)
- Verbindliches Berechtigungsvergabeverfahren
- Es existiert ein Administrationskonzept zur nachvollziehbaren Beantragung und Vergabe der Zugriffsrechte
- Erkennung und Unterbindung von wiederholten, fehlgeschlagenen Anmeldeversuchen, um Brute-Force-Angriffe abzuwehren
- Protokollierung der Veränderung von Berechtigungen
- Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung der Geschäftsführung)
- Dokumentation der Netzlaufwerkzugriffe für berechtigte Benutzer(-gruppen)

- Berechtigungskonzept ist dokumentiert
- Vergabe minimaler Berechtigungen (Need-to-know-Prinzip)
- Die Vergabe von generischen Gruppenkennungen oder Passwörtern ist in der Software nicht vorgesehen und wird nicht empfohlen.
- Die Software erlaubt die Vermeidung der Konzentration von Funktionen und ermöglicht die Funktionstrennung von Administrationstätigkeiten auf unterschiedliche qualifizierte Personen.
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger durch Serverdienstleister

1.4 Pseudonymisierung

Auswertungen werden pseudonymisiert, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist

1.5. Anonymisierung

Alle Daten, die im Sinne der Ziffer 4.2 anonymisiert werden, werden so verarbeitet, dass es nicht möglich ist, sie einer echten Person zuzuordnen. Die anonymisierten Daten werden in einer gesonderten abgegrenzten Datenbank gespeichert. Mit diesem technischen Vorgehen ist gewährleistet, dass ein Personenbezug nicht nachträglich wiederhergestellt werden kann.

1.6 Trennungskontrolle

- Die in den verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzepts.
- Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Mandanten Rechnung trägt.
- Kennzeichnung der erfassten Daten (Aktenzeichen, ID, Kunden-/Vorgangsnummer)
- Funktionstrennung/Produktion/Test

2. **Integrität**

2.1 Weitergabekontrolle

- Protokollierung der Datenübermittlungen
- Gesicherte Transportprotokolle (SSL, TLS, SFTP)
- Es gilt das Verbot der Nutzung privater Datenträger am Arbeitsplatz
- Papier- und Datenträger mit personenbezogenen Daten werden durch ein qualifiziertes Entsorgungsunternehmen datenschutzgerecht entsorgt.

- Grundsätzlich keine Nutzung mobiler Datenträger. Sofern jedoch notwendig, Nutzung von verschlüsselten mobilen Datenträgern.
- Ein- und ausgehende Datenströme werden durch eine aktuelle/dem technischen Standard entsprechende Firewall-Lösung gefiltert.
- Vereinbarung/Richtlinie zum Einsatz unternehmensfremder Hardware für Zwecke des Unternehmens.
- Vereinbarung/Richtlinie zum Einsatz von Unternehmens-Hardware im privaten Umfeld

2.2 Eingabekontrolle

- Berechtigungskonzept
- Einsatz von Application-Level-Firewalls und Intrusion-Detection-Systemen zur Verhinderung und Erkennung von Angriffen
- Die organisatorische Festlegung der Zuständigkeiten für die Eingabeberechtigten ist dokumentiert.
- Jeder Mitarbeiter hat nur den erforderlichen Zugriff auf die im Rahmen seiner Funktion/Rolle erforderlichen Daten (Prinzip der minimalen Rechte).
- Berechtigungsvergaben auf schützenswerte Ressourcen werden nachvollziehbar nur durch hierfür autorisierte Personen beantragt und vergeben.

2.3 Auftragskontrolle

- Der Vertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Dienstleister außerhalb des schriftlich formulierten Auftrags.
- Der Vertrag enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Der Dienstleister hat einen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Verträge zur Auftragsdatenverarbeitung mit allen relevanten Subunternehmern liegen vor oder sind zumindest beantragt.
- Die eindeutige Vertragsgestaltung, Angebot und Auftragsbestätigung liegen vor.
- Die Auftragserteilung ist formalisiert erfolgt (Auftragsformular)
- Alle zugriffsberechtigten Mitarbeiter sind nachweislich auf das Datengeheimnis verpflichtet.
- Jeder Mitarbeiter hat Arbeitsanweisungen/Richtlinien oder Merkblätter erhalten, die über Maßnahmen zur Einhaltung des Datenschutzes sowie der IT-Sicherheit

informieren.

- Bei Fehlern hinsichtlich der Datenverarbeitung oder Verstoß gegen den Datenschutz erfolgt unverzügliche Information an den Auftraggeber.

3. Verfügbarkeit und Belastbarkeit

- Backup-Verfahren/regelmäßige Sicherungskopien
- Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung
- Backups werden in einem anderen Brandabschnitt als die Quellsysteme gesichert und getrennt verschlüsselt
- Regelmäßige Kontrolle des Zustandes und der Kennzeichnungen von Datenträger für Datensicherungen
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Einsatz von Schutzprogrammen (Virens Scanner/Firewall)
- Monitoring aller relevanten Server
- Proaktive Erkennung von anomalen Verhalten und Events auf allen relevanten Server

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Alle Mitarbeiter wurden schriftlich auf das Datengeheimnis verpflichtet und unterwiesen.
- Alle Mitarbeiter haben einmal pro Kalenderjahr eine Datenschutzbildung (eLearning) zu absolvieren.
- Nachweis über den Erfolg der Schulung durch ein entsprechendes Zertifikat.

Anlage 2 - Unterauftragsverarbeiter

Unterauftragsverarbeiter	Beschreibung der Leistungen	Datenstandort
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	Hosting Straiv Software	EU
Hetzner Online GmbH Industriestr. 2 91710 Gunzenhausen Germany	Hosting Website	EU
LINK Mobility Austria GmbH Brauquartier 5/13 8055 Graz Austria	SMS Distribution	EU
Mailgun Technologies SAS 13-13 bis rue de l'Aubrac 75012 Paris France	E-Mail Distribution	EU
Bird B.V. Keizersgracht 268 1016 EV Amsterdam Netherlands	Whatsapp Messaging	EU
Datadog Inc. 4th Floor, 1 Dockland Central, Guild Street Dublin 1, D01 E4X0 Ireland	Log-Auswertung	EU
Atlassian B.V. Singel 236, 1016 AB Amsterdam Netherlands	Ticket System	EU
Google Cloud EMEA Limited 4th Floor, 1 Dockland Central, Guild Street Dublin 1, D01 E4X0 Ireland	Google Workspace Bereitstellung Chatbot	EU
WhatsApp Ireland Limited Merrion Road Dublin 4, D04 X2K5 Ireland	Whatsapp Distribution	EU
Hubspot Ireland Limited 1 Sir John Rogerson's Quay Dublin 2, D02 CR67 Ireland	Kundenkommunikation	EU
OpenAI Ireland Ltd The Liffey Trust Centre, 117-126 Sheriff Street Upper Dublin 1, D01 YC43 Ireland	Bereitstellung Chatbot	EU

LangChain Inc. Office 2 12A Lower Main Street, Lucan Co. Dublin Ireland	Bereitstellung Chatbot	EU
n8n GmbH Novalisstr. 10 10115, Berlin Germany	Prozessautomatisierung	EU

Stand: 30.03.2026

Version: 1.7