bookingkit

Vereinbarung zur Auftragsverarbeitung

Data Processing Agreement

VEREINBARUNG zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

DATA PROCESSING AGREEMENT in accordance with art. 28 GDPR

Zwischen

– Verantwortlicher, nachstehend Auftraggeber genannt –

und

between

– Controller, hereinafter called the Client -

and

bookingkit GmbH
vertreten durch / *represented by* Christoph Kruse und Lukas C. C. Hempel
Sonnenallee 223
D-12059 Berlin

– Auftragsverarbeiter, nachstehend Auftragnehmer genannt –

– the contract processor, hereinafter called the Supplier –

IMPORTANT NOTE: Only the original German-language version of this contract is legally binding. The English translation is provided for information purposes only.

Definitionen

Die nachfolgend aufgeführten Begriffe haben für diesen Vertrag die ihnen daneben zugeordnete Bedeutung, soweit sich aus dem Kontext nicht ausdrücklich etwas anderes ergibt:

"bookingkit Plattform":
Die Gesamtheit der Dienste des Auftragnehmers

„Drittländer“:
Länder außerhalb der EU/ des EWR

Definitions

The following terms have the specified meanings for this contract, unless expressly stated otherwise due to the context:

"bookingkit platform":
The entirety of services provided by the Supplier

„Third countries“:
Countries outside of the EU/the EEA

1

Gegenstand und Dauer des Auftrags

(1) **Gegenstand**
Gegenstand des Auftrags zum Datenumgang ist die Durchführung

1

Object and duration of the Agreement

(1) **Object**
The object of the Agreement on data handling is for the following tasks to

folgender Aufgaben durch den Auftragnehmer: Verarbeitung von personenbezogenen Daten im Bereich SAAS Tool (bookingkit Plattform) zur Erfüllung der vom Auftraggeber bezahlten Leistungen im Bereich Vermarktung, Verwaltung und Verkauf seiner Angebote

be performed by the Supplier: processing personal data in the area of SAAS Tool (the bookingkit platform) to fulfil the services paid for by the Client in the area of marketing, managing and selling its offers.

(2) **Dauer**
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der bestehenden Leistungsvereinbarung.

(2) **Duration**
The duration of this Agreement (term) corresponds to the term of the existing Service Agreement.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

(3) Amendments and supplements to this Agreement and all its components - including any assurances by the Supplier - shall require an agreement in writing or in an electronic format which contains an express reference to the fact that this Agreement has been amended or supplemented.

2

Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der vorgesehenen Verarbeitung von Daten**

- Zweck 1 - Geschäftsmodell des Auftraggebers darstellen / Angebot des Dienstes:

  Technische Lösung, um das Geschäftsmodell des Auftraggebers abbilden zu können; dies beinhaltet sowohl die Erstellung von Erlebnissen auf der bookingkit Plattform als auch die technische Abbildung der Konditionen, des gewünschten Buchungsvorganges, des Kommunikationsprozesses mit den Endkunden und zusätzlicher Unternehmensprozesse des Verantwortlichen

- Zweck 2 - Verwaltung des Treuhandkontos:

2

Specific details as to content of agreement

(1) **Type and purpose of planned data processing**

- Purpose 1 - representation of the Client's business model/offer of service:

  Technical solution aimed at mapping the Client's business model; this includes both creating Experiences on the bookingkit platform and also technical mapping of the conditions, desired booking procedure, communication process with end customers and additional business processes of the party responsible.

- Purpose 2 - management of trustee account:

Verwaltung des Treuhandkontos des Auftraggebers, um Zahlungen für ihn zu akzeptieren und Auszahlungen zu verarbeiten;

- Zweck 3 - Übermittlung von Informationen zu Diensten des Auftragnehmers:

  Informationen über Änderungen der Dienste des Auftragnehmers übermitteln, die dem Auftraggeber dazu dienen, sein Geschäft effizienter/effektiver abzuwickeln.

- Zweck 4 - Hilfestellung Service-Team:

  Direkte Hilfestellung für die Dienste des Auftragnehmers durch sein Serviceteam auf Anfrage des Auftraggebers oder proaktiv sollte Handlungsbedarf durch den Auftragnehmer festgestellt oder empfohlen sein.

- Zweck 5 – Ermöglichung der Vermarktung über Partner

  Technische Lösung, um dem Auftraggeber zu ermöglichen, seine Angebote mithilfe ausgewählter Partnerunternehmen zu vermarkten. Hierzu kann der Auftraggeber die Weitergabe seiner Kontaktdaten und die Daten der von ihm angebotenen Erlebnisse an entsprechende Partner veranlassen, sofern er mit diesen zusammenarbeiten möchte, so dass der Partner mit dem Anbieter für eine Vertragsanbahnung in Kontakt tritt.

- Zweck 6 – Speicherung von Identitätsnachweisen

  Zum Zwecke des vertragsgemäßen Anlegens von Treuhandkonten und zur Ermöglichung der Zusammenarbeit mit Zahlungsanbietern im Rahmen der Vertragserfüllung in Anlehnung an § 11 Geldwäschegesetz sowie zum Zwecke des Nachweises von Prüfungen von hoheitlich erstellten Sanktionslisten.

Management of trustee account belonging to the Client to accept payments for it and process outgoing payments;

- Purpose 3 - communication of information regarding the services provided by the Supplier

  Communicating information about changes to the services provided by the Supplier, which the Client can use to run its business more efficiently/effectively;

- Purpose 4 - support by service team:

  Direct assistance for the services provided by the Supplier provided by the service team on request by the Client or proactively if a need for action is established or recommended by the Supplier.

- Purpose 5 – allowing for marketing by partners

  Technical solution allowing the Client to market its services via selected partner companies.
  For this purpose, the Client may agree to his contact data and the data concerning the experiences which the Client offers being passed on to relevant parties, provided the Client wishes to collaborate with them, so that the partner may make contact with the provider for the purposes of contract initiation.

- Purpose 6 – storing proofs of identity

  For the purpose of creating trustee accounts in accordance with the contract and to facilitate collaboration with payment providers within the scope of contract fulfilment pursuant to § 11 of the Money Laundering Act as well as for the purpose of providing evidence of checks of sanctions lists created by the authorities.

(2) **Art der Daten -** Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Angaben zur Person:
  - Name
  - Anschrift
  - Geburtsdatum
  - Email Adresse
  - Telefonnnummer
  - Ggf. IBAN
  - Ggf. BIC
  - Ggf. Firmenname
  - Ggf. Steuernummer
  - Ggf. Kopie des Lichtbildausweises
- Online-bezogene Daten:
  - Cookie/ Sitzungsidentifikationsnummer
  - IP Adresse (zur Identifikation bei Vertragsabschluss)
  - Zeitstempel
  - Login-Daten
- Kundendaten:
  - Name
  - E-Mail Adresse
  - Zahlungsart

(3) **Kategorien betroffener Personen** - Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Angestellte
- Auszubildende
- Gewerbliche Mitarbeiter
- Interessenten
- Kunden
- Mitarbeiter
- Praktikanten
- User

(2) **Type of data -** the object of personal data processing are the following types/categories:

- Details of person:
  - Name
  - Address
  - Date of Birth
  - Email address
  - Tel. no.
  - IBAN (if applicable)
  - BIC (if applicable)
  - Company name (if applicable)
  - Tax number (if applicable)
  - Copy of photo ID (if applicable)
- online-related data:
  - Cookie / session ID
  - IP address (for identification when Agreement signed)
  - Time stamp
  - Login data
- Customer data:
  - Name
  - Email address
  - Type of payment

(3) **Categories of affected persons -** the categories of persons affected by processing are:

- Clerical workers
- Trainees
- Industrial employees
- Interested parties
- Customers
- Employees
- Interns
- Users

3

Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet,

3

Technical-organisational measures

(1) The Supplier must document implementation of the necessary technical and organizational measures presented before the contract was awarded before the start of processing, in particular relative to specific implementation of the Agreement, and hand this to the Client for inspection. When the Client accepts these, the documented measures become the basis of the Agreement. Should any inspection/an audit by the Client reveal the need for revision, this must be implemented by joint agreement.

(2) The Supplier must provide security in accordance with 28 para. 3 letter c, 32 GDPR in particular in conjunction with art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are measures aimed at data security and to guarantee a protection level which is appropriate to the risk in respect of the confidentiality, integrity, availability and resilience of the systems. The current state of the art, implementation costs and the type, scope and purposes of processing, as well as the different probability of the risk occurring and its seriousness in respect of the rights and freedoms of natural persons must be taken into account as defined in art. 32 para. 1 GDPR [Details in Appendix 1].

(3) The technical and organizational measures are subject to technical progress and development. To this extent the Supplier is permitted to implement suitable alternative measures. In so doing, falling short of

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

the measures specified is not permitted. Any major changes must be documented.

4

Berichtigung, Einschränkung und Löschung von Daten

(1) 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. Die Weisung muss schriftlich erfolgen über die Emailadresse datenschutz@bookingkit.de. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

4

Correction, restriction and deletion of data

(1) The Supplier may not itself correct or delete the data processed under contract, nor limit their processing, except in accordance with a documented instruction from the Client. These instructions must be given using the email address dataprotection@bookingkit.de. If a person affected makes a request directly to the Supplier in this respect, the Supplier will forward the request to the Client immediately.

(2) If covered by the scope of supply, the deletion concept, right to be forgotten, correction, data portability and information must be provided directly by the Supplier after receipt of a documented instruction from the Client.

5

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine

5

Quality assurance and other duties of the Supplier

In addition to observing the regulations of the Agreement, the Supplier has statutory duties in accordance with arts. 28 to 33 GDPR; to this extent it guarantees in particular that it will comply with the following requirements:

a. written order from a data protection officer who is exercising

Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer die ePrivacy GmbH vertreten durch Prof. Dr. Christoph Bauer, Große Bleichen 21, 20354 Hamburg, telefonisch zu erreichen unter +49 (0) 40 609451810 und per E-Mail über datenschutz@bookingkit.de bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die während des Auftrags und nach dessen Beendigung auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
d. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder

its duty under arts. 38 and 39 GDPR.

The Supplier's data protection officer is ePrivacy GmbH, represented by Dr. Christoph Bauer, Große Bleichen 21, 20354 Hamburg, who can be contacted by telephone on +49 (0) 40 609451810 and by email at dataprotection@bookingkit.de. The Client must be informed immediately of any change in the data protection officer.

b. Maintenance of confidentiality in accordance with arts. 28 para. 3 S. 2 letter b, 29, 32 para. 4 GDPR. In performing its work, the Supplier will use, within duration of the contract and after its completion, only employees who have undertaken to maintain confidentiality and have been previously made familiar with the relevant conditions on data protection. The Supplier and every person subordinate to the Supplier who has access to personal data must process these data exclusively in accordance with the Client's instructions, including the powers granted under this Agreement, unless they have a legal obligation to process them.
c. The implementation and fulfilment of the technical and organizational measures necessary for this Agreement in accordance with arts. 28 para. 3 p. 2 letter c, 32 GDPR [Details in Appendix 1].
d. The Client and the Supplier will work together with the supervisory authority on request to fulfil their tasks.
e. Immediate information to be provided by the Client on monitoring actions and measures taken by the supervisory authority, to the extent that they relate to this

Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f. 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.

g. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

Agreement. This also applies if a competent authority investigates order processing by the Supplier as part of proceedings related to regulatory offences or criminal proceedings associated with the processing of personal data.

f. If the Client for its part is subjected to monitoring by the supervisory authority, proceedings for infringement or criminals proceedings, a liability claim from a person affected or a third party, or another claim in connection with the order processing by the Supplier, the Supplier must support it to the best of its ability.

g. The Supplier will regularly monitor the internal processes, technical and organizational measures to guarantee that the processing within its area of responsibility complies with the requirements of applicable data protection law, and that protection of the rights of the person affected is guaranteed.

h. Demonstrability of technical and organizational measures taken in respect of the Client within the context of its supervisory powers under section 7 of this Agreement.

6

Unterauftragsverhältnisse

(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 Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und

6

Sub-contract arrangements

(1) Sub-contract arrangements as defined in this clause are to be understood as services which relate directly to the provision of the main service. They do not include incidental services which the Supplier use for instance as telecommunication services, post/transport services, maintenance and user service or the disposal of data supports, and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software in data processing

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.

installations. The Supplier nevertheless has a duty to enter into reasonable contractual agreements which comply with the law and supervisory measures to guarantee data protection and the security of the Client's data, including for incidental outsourced services.

(2) Die Auslagerung auf Unterauftragnehmer und der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt, wobei die Anzeige auch durch Vorab-Aktualisierung des Anhangs 2 dieser Vereinbarung geschehen kann, welche durch den Auftraggeber in regelmäßigen Abständen geprüft wird, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben, und
- die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Outsourcing to sub-contractors and changing existing sub-contractors are permitted if:

- the Supplier informs the Client of any intention to outsource to subcontractors with an appropriate notice period in written form or in text form; such an indication may also take place by pre-updating Appendix 2 of this agreement, which is checked at regular intervals by the Client, which gives the Client a possibility of objecting to such changes and
- the particular prerequisites of art. 44 et seq. GDPR are met.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(3) Forwarding the Client's personal data to the sub-contractor and an activity being taken for the first time by the latter are permitted only when all pre-conditions for a sub-contract have been met.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(4) If the sub-contractor provides the agreed service outside the EU/the EEA, the Supplier will guarantee the admissibility of this under data protection law by taking the appropriate measures. The same applies if service-providers are to be used as defined in para. 1 sentence 2.

(5) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch den Unterauftragnehmern aufzuerlegen.

(5) All contractual regulations in the contract chain must also be imported on the sub-contractors.

7

Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

7

Client's right of inspection

(1) The Client has the right, in consultation with the Supplier, to carry out inspection visits or to arrange for such inspection to be carried out in an individual case by named inspectors. He has the right to convince itself by means of random checks, which are generally to be notified in good time, that the Supplier is complying with this Agreement on its business premises.

(2) The Supplier shall ensure that the Client is able to convince itself that the Supplier is fulfilling its duties under art. 28 GDPR. The Supplier undertakes to provide the Client with the necessary information on request, and in particular to prove that it has implemented the technical and organisational measures.

(3) The proof of such measures, which affect not only the specific contract, may be provided by

- compliance with approved rules of conduct as set out in art. 40 GDPR;
- certification in accordance with an approved certification procedure as set out in art. 42 GDPR;
- current certificates, reports or excerpts from reports by independent bodies (e.g. auditors, data protection officers, IT security department, data protection auditors, quality auditors;

- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

- suitable certification by IT Security or Data Protection audit (e.g. in accordance with BSI basic protection).

(4) The Supplier is entitled to pursue a claim for remuneration for making such checks by the Client possible.

8

Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

8

Notification in the event of infringement by the Supplier

(1) The Supplier supports the Client in compliance with the duties to safeguard personal data, duties of notification of data breaches, data protection impact assessments and prior consultation required under articles 32 to 36 of GDPR. This includes, amongst other things,

a. ensuring a reasonable level of protection through technical and organisational measures, which take into account the circumstances and purpose of processing, and the predicted probability and seriousness of possible infringement of the law due to security breaches, and make immediate detection of relevant infringement incidents possible

b. the duty to notify the Client immediately of breaches of personal data

c. the duty to support the Client within the context of its duty to provide information to an affected person and to make all relevant information available to it immediately in connection with this

d. support for the Client in compiling its data protection impact assessment

e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen, sofern nicht die Vergütung durch Gesetz dem Auftragnehmer auferlegt wird.

e. support for the Client within the context of prior consultations with the supervisory authorities.

(2) For support services which are not included in the description of services or cannot be attributed to wrongdoing on the part of the Supplier, the Supplier may claim remuneration, unless the remuneration is imposed on the Supplier by law.

9

Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9

Client's authority to give instructions

(1) The Client must confirm verbal instructions immediately (as a minimum in text form)

(2) The Supplier must inform the Client immediately if it is of the opinion that an instruction would breach data protection regulations. The Supplier is entitled to suspend action on such an instruction until this is either confirmed or revised by the Client.

10

Löschung und Rückgabe von personenbezogenen Daten

(1) 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

10

Secrecy

(1) No copies or duplicates of the data will be compiled without the Client's knowledge. This provision excludes back-up copies to the extent that these are necessary to guarantee proper data processing, and data which are necessary for the purpose of complying with statutory duties to store them.

Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ausgenommen sind Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, welche der Auftragnehmer aufgrund rechtlicher Bestimmungen aufzubewahren hat.

(2) After completion of the contractually agreed work, or earlier at the request of the Client (but at the latest when the Agreement on Services ends), the Supplier must hand over to the Client all the documents which have come into its possession, as well as all results derived from the processing and usage of the data which it has obtained or generated respectively in relation to the contractual relationship or delete or destroy such materials in accordance with data protection regulations. The same applies to test and defective material. The deletion protocol must be presented on request. Exceptions to this rule are documents, compiled results of processing and use as well as data sets associated with the contractual relationship that the Supplier is obligated to store due to legal provisions.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(3) Documentation used to prove that data processing has been carried out in accordance with the contract and correctly is to be stored by the Supplier beyond the end of the Agreement in accordance with the respective retention periods. To relieve it of this duty, it may hand this over to the Client at the end of the contract.

ANLAGE 1
Technisch-organisatorische Maßnahmen

1

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

a. Zutrittskontrolle

- Der Auftragnehmer stellt anhand von elektronischen Schlüsseln sicher, dass nur autorisierte Personen Zutritt zu ihren Räumlichkeiten haben. Diese können individuell gesperrt werden.
- Außerdem ist das Bürogelände des Auftragnehmers 24 Stunden täglich von einem Wachdienst geschützt, welcher regelmäßig Rundgänge durchführt.
- Es ist ein Alarmsystem installiert, welches mit einem Schließmechanismus für die Türen gekoppelt ist.
- Die Tür des Serverraums ist mit einem Schlüssel gesichert, welcher nur dem zuständigen Personal zur Verfügung steht.
- Mitarbeitern im Homeoffice ist es untersagt, außerhalb des Bürogeländes betriebliche Unterlagen auf Papier oder portablen Datenträgern zu nutzen. Daten sind ausschließlich über die zentrale Datenverwaltung zu nutzen.

b. Zugangskontrolle

- Der Auftragnehmer gewährt Mitarbeitern nur auf die Systeme Zugriff, welche er für die Ausführung seiner konkreten Aufgaben benötigt.
- Den Zugang zu den eigenen Systemen regelt der

APPENDIX 1
Technical-organizational measures

1

Confidentiality
(art. 32 para. 1 letter b GDPR)

a. Physical access control

- The Supplier ensures by means of electronic locks that only authorised persons have access to its premises. These can be individually locked.
- The office site of the Supplier is furthermore protected by security guards 24/7, and they carry out regular patrols.
- An alarm system has been installed which is linked to a locking mechanism for the doors.
- The door of the server room is secured by a key which is only available to responsible staff.
- Employees in the home office are prohibited from using company documents on paper or portable data storage devices outside the office premises. Data may only be used via the central data management system.

b. Computer access control

- The Supplier only grants employees to the systems which it needs to carry out its specific tasks.
- The Supplier regulates access to its own systems via secure personalized passwords and

Auftragnehmer über sichere personalisierte Passwörter und Passwortverfahren. Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account geknüpft. Außerdem verfügen alle Mitarbeiter des Auftragnehmers über ein Passwortmanagementsystem, welches im Bedarfsfall zufällige Passwörter für sensible Systeme festlegt.

- Passwörter des Auftragnehmers unterliegen Mindestanforderungen an Sicherheitsbestimmungen.
- Alle Datenträger und Laptops sind verschlüsselt.
- Alle Windows Laptops nutzen die Full Disk Hardware Encryption der verbauten SSDs. Alle Macbooks nutzen die integrierte Filevault Encryption von MacOS.
- Alle Computer verfügen über Virenscanner, welche täglich geupdated werden.

c. Zugriffskontrolle

- Zugangsberechtigte können nur auf Daten zugreifen, die in ihrem individuellen Berechtigungsprofil eingerichtet sind.
- Zum Erstellen und Ändern von Berechtigungsprofilen gibt es strenge Regelungen und Verfahren, welche die Genehmigung durch die Geschäftsführung einschließen.
- Das Sperren bzw. Abmelden beim Verlassen des Arbeitsplatzes ist schriftlich angeordnet und wird praktiziert.
- Alle Server und Services des Auftragnehmers werden kontinuierlich überwacht.

d. Trennungskontrolle

- Berechtigungskonzepte verhindern die ungeplante

password procedures. Authorizations are linked to a personal user ID and an account. All of the Supplier's employees also have a password management system available to them, which if necessary sets randomly generated passwords for sensitive systems.

- Supplier passwords are subject to the minimum requirements for safety regulations.
- All data carriers and laptops are encrypted.
- All Windows laptops use the Full Disk Hardware Encryption of the built-in SSDs. All Macbooks use the integrated Filevault Encryption of the MacOS.
- All computers have virus scanners which are updated daily.

c. Data access control

- Persons with authorized access can only access data which are set up in their individual authorization profile.
- There are strict rules and procedures for creating and changing authorization profiles which include approval by senior management.
- There is a written order to the effect that access must be blocked/logged out when a user leaves the workstation, and this is put into practice.
- All of the Supplier's servers and services are continuously monitored.

d. Separation control

- Authorization concepts prevent the unplanned use of sensitive

Verwendung sensibler Daten. Der Zugriff auf die Daten selbst ist zudem dadurch eingeschränkt, dass die Mitarbeiter Services (Applikationen) verwenden, welche den Zugriff steuern und kein Beschreiben der Daten zulassen.

- Alle Kundendaten werden in der selben Datenbank verwaltet, da es systembedingt nicht möglich ist diese auf Datenbankebene zu trennen. Da ohnehin ausschließlich über entsprechende Software auf die Daten zugegriffen werden darf, wird Trennung über ein Rollenkonzept in der Software sichergestellt.
  Ausnahmen gelten für Developer und das Customer Success Team, die zur Fehlerbehebung direkt auf die Datenbank zugreifen dürfen. Dieser Zugriff erfolgt ausschließlich lesend, so dass keine Daten am Rollenkonzept vorbei verändert werden können.
- Es gibt ein abgetrenntes WLAN für Gäste.
- Es erfolgt eine Trennung von Test- und Produktivsystemen. Sollten Softwareneuerungen der Trennungskontrolle nicht genügen, werden diese im Testsystem aufgedeckt und nicht in das Produktivsystem übernommen.

e. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Daten für interne Auswertungen zu statistischen Zwecken zur Produktivitätssteigerung werden vor der Verarbeitung anonymisiert indem die IP Adressen gekürzt bzw. zufällig verändert werden.
- Insbesondere im Bereich des Onlinemarketings wird ausschließlich mit pseudonymen Online-Identifiern und -Profilen gearbeitet. Diese werden mittels des sogenannten hashings pseudonymisiert

data. Access to the data themselves is further restricted by the fact that staff use services (Apps) which control access and do not permit data to be written.

- All customer data are managed in the same database, as it is not possible for system reasons to separate these into database levels. As access to the data is in any case only possible via the corresponding software, separation is safeguarded by a role concept in the software. Exceptions apply to developers and the Customer Success Team which are allowed direct access to the database for debugging. This access is read-only, so that no data can be changed by bypassing the role concept.
- There is a separate WLAN for visitors.
- There is separation of test and productive systems. If software innovations do not satisfy separation control requirements, these will be discovered in the test system and not included in the productive system.

e. Anonymizing (art. 32 para. 1 letter a GDPR; art. 25 para. 1 GDPR)

- Data for internal analysis used for statistical purposes to improve productivity will be anonymized before processing by abbreviating or randomly changing the IP addresses.
- Particularly in the area of online marketing, exclusively anonymized online identifiers and profiles are used for processing. These are anonymized by “hashing”.

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

a. Weitergabekontrolle

- Alle Transportwege sind SSL-verschlüsselt.
- Das Rechtemanagement für die Datenauslesung des Auftraggebers liegen beim Auftraggeber.
- Der Verkehr zwischen den Systemen ist über SSL/TLS verschlüsselt.
- Das Frontend verfügt über eine Https-Verschlüsselung.
- Der Zugang zu den Systemen von außen ist über open VPN verschlüsselt. Mitarbeiter mit VPN Zugang müssen sich über Benutzername/Passwort und ein Zertifikat authentifizieren.
- Hardwarekomponenten oder Dokumente werden so vernichtet, dass eine Wiederherstellung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.
- Die Datenübertragung zwischen Clients und Servern erfolgt verschlüsselt.
- Für die Anfertigung von Kopien gibt es eindeutige Regelungen und Verfahrensweisen.
- Es existieren mehrere Firewalls.
- Auf sämtlichen Arbeitsstationen existieren Firewalls, welche ständig aktiviert sind und durch den Nutzer nicht deaktivierbar sind.

b. Eingabekontrolle

- Die Mitarbeiter außerhalb der Entwicklungsabteilung des Auftragnehmers arbeiten nicht direkt auf Datenbankebene, sondern nutzen Applikationen, um auf die Daten zuzugreifen.
- Datenbankstrukturänderungen werden detailliert im

2

Integrity
(art. 32 para. 1 letter b GDPR)

a. Forwarding control

- All transmission paths are SSL encrypted.
- Rights management for reading data from the Client's data is the responsibility of the Client.
- Traffic between the systems is encrypted via SSL/TLS.
- The frontend has HTTPS encryption.
- Access to the systems from outside is encrypted via open VPN. Staff with VPN access must authenticate themselves via user name/password and a certificate.
- Hardware components or documents are destroyed in such a way that restoration is not possible, or only with disproportionate effort.
- Data transmission between Clients and Servers is in encrypted form.
- There are clear rules and procedures for making copies.
- Several firewalls exist.
- Firewalls exist on all workstations which are continuously activated and cannot be deactivated by users.

b. Input control

- Staff outside the Supplier's development department does not work directly at database level but uses applications to access the data.
- Database structure changes are recorded in detail in the project

Projektmanagementtool JIRA protokolliert. Die Protokolle werden revisionssicher 12 Monate lang aufbewahrt. Die Eingabe, Änderung und Löschung von Daten kann dabei anhand von individuellen Benutzernamen nachvollzogen werden.

- IT-Mitarbeiter verwenden einen gemeinsamen Login für die Datenbanken, da es wenige Mitarbeiter sind, die räumlich beieinander sitzen. Durch Absprachen und Sichtkontrollen wird die Arbeit an den Datenbanken zusätzlich überwacht.

management tool JIRA. The protocols are retained for 12 months and are tamper-proof. Data input, modification and deletion can be undertaken by individual user names.

- IT staff use a joint login for the databases, as there are few staff who sit next to one another. Work on the databases is further monitored by consultation and visual inspection.

3

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

Verfügbarkeitskontrolle

- Der Auftragnehmer erstellt täglich ein weiteres Gesamt-Backup, welches für 7 Tage gespeichert wird. Auf diese Backups kann zurückgegriffen werden, sollten andere Verfügbarkeitsmaßnahmen versagen. Es handelt sich hierbei um ein Gesamtbackup, welches nicht zur Wiederherstellung einzelner Daten herangezogen werden kann, sondern lediglich das komplette System wiederherstellt.
- Aus diesen Backups kann jederzeit im Falle eines Notfalls das System wiederhergestellt werden.
- Es existiert ein Notfallplan, aus welchem hervor geht, welche Schritte wann eingeleitet werden müssen und welche Personen und Stellen zu welchem Zeitpunkt und welchem Zweck informiert werden müssen.
- Die einzelnen Arbeitsstationen beim Auftragnehmer sind über täglich

§ 3

Availability and resilience (art. 32 para. 1 letter b GDPR)

Availability control

- The Supplier carries out an additional overall backup on a daily basis, which is saved for 7 days. These backups can be used if other measures to safeguard availability fail. These are overall backups that cannot be used to retrieve individual pieces of data, but instead simply restore the entire system.
- The system can be restored from these backups at any time in an emergency.
- There is an emergency plan which stipulates what steps are to be taken when, and which people and which department must be informed at what stage and for what purpose.
- The Supplier's individual workstations are protected by virus scans updated daily, data supports are encrypted.

geupdatete Virenscans geschützt, die Datenträger sind verschlüsselt.

- Unsere Server und Backup-Systeme stehen in den Rechenzentren von Amazon Web Services welche umfassend für die Betriebskontinuität geschützt sind. Details dazu können sie hier nachlesen: https://aws.amazon.com/de/compliance/data-center/controls/
- Hochverfügbare Systeme werden parallel in mehreren Rechenzentren redundant betrieben.
- Die Überlastung von Servern ist durch eine sogenannte autoscaling group ausgeschlossen. Steigt die Last auf die Server werden automatisiert weitere Server hinzu geschaltet, um eine Überlastung zu verhindern.
- Sämtliche Betriebsparameter werden permanent überwacht.

- Our server and backup systems are located in the computer centers of Amazon Web Services, which are comprehensively protected for operational continuity. You can find more details about this at: https://aws.amazon.com/de/compliance/data-center/controls/
- High-availability systems are run on a redundant basis in parallel in several computer centers.
- Overloading of services is excluded by autoscaling group. If the load on the server rises, further servers will be automatically connected to prevent an overload.
- All operating parameters are permanently monitored.

4

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

a. Datenschutz Management
   - Der Auftragnehmer überprüft regelmäßig ihr Datenschutz-Management unter Einbeziehung des betrieblich bestellten Datenschutzbeauftragten.
   - Sämtliche Mitarbeiter werden regelmäßig zum Thema Datenschutz geschult. Außerdem werden alle Mitarbeiter auf das Datengeheimnis verpflichtet. Mitarbeiter im Homeoffice werden auf die besonderen Regeln gesondert belehrt.

b. Incident Response Management
   - Im Falle einer Datenpanne greift ein umfassendes Regelwerk zu

4

Procedure for regular checking, assessing and evaluating (art. 32 para. 1 letter d GDPR; art. 25 para. 1 GDPR)

a. Data protection management
   - The Supplier regularly checks its data protection management using the data protection officer appointed by the company.
   - All staff are regularly trained on the subject of data protection. And all staff also give an undertaking to maintain data secrecy. Employees in the home office are instructed separately on the special rules.

b. Incident Response Management
   - In the event of a data breach, a comprehensive procedure is

einzuleitenden Prozessen und Kommunikationsschritten.

- Für die gegebenenfalls zu erfolgende Information von Aufsichtsbehörden sind die verantwortlichen Mitarbeiter geschult, so dass einer Information innerhalb von 72 Stunden nichts im Wege steht.

c. Datenschutzfreundliche Voreinstellungen

- Bei der Entwicklung jeder Technologie oder jedes neuen Produktes wird von vornherein ein Privacy by Design-Ansatz verfolgt. Es wird von vornherein das Ziel verfolgt, die Menge der zu erhebenden Daten zu minimieren und den Umfang der Datenverarbeitung zu reduzieren
- Soweit möglich werden Daten nur pseudonymisiert weiterverarbeitet. Datenschutzerklärungen, welche leicht zugänglich sind und sämtliche Datenprozesse ausführlich beschreiben, sorgen für Transparenz.

d. Auftragskontrolle

- Sämtliche Auftragnehmer sind unter Sorgfaltsgesichtspunkten ausgewählt.
- Mit sämtlichen Auftragnehmers werden Auftragsverarbeitungsverträge abgeschlossen und technische und organisatorische Maßnahmen werden regelmäßig überprüft.
- Kontrollrechte werden mit Auftragnehmern vertraglich vereinbart.

invoked on processes to be instigated and steps in communication.

- The staff responsible are trained in providing information to the supervisory authorities if need be, so that there is no obstacle to providing information within 72 hours.

c. Default settings which are data-protection friendly

- In the development of any technology or new product, a Privacy by Design approach is taken from the outset. From the outset, the aim of minimizing the quantity of data to be collected and reducing the scope of data processing is pursued.
- As far as possible, data are only further processed in anonymized form. Data protection declarations which are easy to access and describe all data processes in detail ensure transparency.

d. Order control

- All suppliers are selected for their diligence.
- Order processing agreements are entered into with all suppliers, and technical and organizational measures are regularly checked.
- Rights of control are contractually agreed with suppliers.

ANLAGE 2
Unterauftrags-verhältnisse

Präambel

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 Auftragnehmer 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.

1

Bestehende Unterauftragsverhältnisse

Eine Liste von bestehenden Unterauftragsverhältnisse ist unter folgendem Link abrufbar: https://bookingkit.net/legaldocuments-dpa-list

APPENDIX 2
Sub-contract arrangements

Preamble

Sub-contract arrangements as defined in this clause are to be understood as services which relate directly to the provision of the main service. They do not include incidental services which the Supplier use for instance as telecommunication services, post/transport services, maintenance and user service or the disposal of data supports, and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software in data processing installations.

1

Existing sub-contract arrangements

List of current sub-contract arrangements can be found under the following Link: https://bookingkit.net/legaldocuments-dpa-list

2

Bestehende Unterauftrags-verhältnisse mit Unternehmen aus Drittländern

Eine Liste von bestehenden Unterauftragsverhältnisse mit Unternehmen aus Drittländern ist unter folgendem Link abrufbar: https://bookingkit.net/legaldocuments-dpa-list-2/

2

Existing sub-contract arrangements with companies from third countries

List of current sub-contract arrangements with companies from third countries can be found under the following Link: https://bookingkit.net/legaldocuments-dpa-list-2

bookingkit

Vertrag zur Auftragsverarbeitung

Contratto relativo alla responsabilità del trattamento dei dati

VEREINBARUNG zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

- Verantwortlicher, nachstehend Auftraggeber genannt –
und

ACCORDO relativo alla responsabilità del trattamento dei dati ai sensi dell'art. 28 RGPD

tra

- Titolare del trattamento, di seguito denominato "Committente" -
e la

bookingkit GmbH
vertreten durch / *rappresentata da* Christoph Kruse e Lukas C. C. Hempel
Sonnenallee 223
D-12059 Berlin

- Auftragsverarbeiter, nachstehend Auftragnehmer genannt -

- Responsabile del trattamento, di seguito denominato "Fornitore" -

Solo la versione originale in lingua tedesca del presente contratto è giuridicamente vincolante. La traduzione in italiano è fornita a titolo puramente informativo.

Definitionen

Die nachfolgend aufgeführten Begriffe haben für diesen Vertrag die ihnen daneben zugeordnete Bedeutung, soweit sich aus dem Kontext nicht ausdrücklich etwas anderes ergibt:

"bookingkit Plattform":
Die Gesamtheit der Dienste des Auftragnehmers

„Drittländer“:
Länder außerhalb der EU/ des EWR

Definizioni

I termini indicati di seguito acquisiscono il significato attribuito accanto per il presente contratto, a meno che non si evinca espressamente qualcos'altro dal contesto:

"Piattaforma bookingkit":
Il complesso dei servizi del Fornitore

„Paesi terzi “:
Paesi al di fuori della UE/dello SEE

1

Gegenstand und Dauer des Auftrags

(1) **Gegenstand**
Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Verarbeitung von

1

Oggetto e durata dell'incarico

(1) **Oggetto**
Oggetto dell'incarico in relazione alla manipolazione dei dati è l'esecuzione delle seguenti attività da parte del Fornitore:

personenbezogenen Daten im Bereich SAAS Tool (bookingkit Plattform) zur Erfüllung der vom Auftraggeber bezahlten Leistungen im Bereich Vermarktung, Verwaltung und Verkauf seiner Angebote

(2) **Dauer**
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der bestehenden Leistungsvereinbarung.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

2

Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der vorgesehenen Verarbeitung von Daten**

- Zweck 1 - Geschäftsmodell des Auftraggebers darstellen / Angebot des Dienstes:

  Technische Lösung, um das Geschäftsmodell des Auftraggebers abbilden zu können; dies beinhaltet sowohl die Erstellung von Erlebnissen auf der bookingkit Plattform als auch die technische Abbildung der Konditionen, des gewünschten Buchungsvorganges, des Kommunikationsprozesses mit den Endkunden und zusätzlicher Unternehmensprozesse des Verantwortlichen

Trattamento di dati personali nell'ambito del SAAS Tool (piattaforma bookingkit) per l'adempimento dei servizi remunerati dal committente nei campi della commercializzazione, della gestione e della vendita delle sue offerte

(2) **Durata**
La durata del presente incarico (durata) corrisponde alla durata dell'accordo attuale sul servizio.

(3) Le modifiche e le integrazioni al presente contratto e a tutti i suoi componenti - comprese eventuali assicurazioni da parte del fornitore - richiederanno un accordo scritto o in formato elettronico che contenga un riferimento esplicito al fatto che il presente contratto sia stato modificato o integrato.

2

Concretizzazione del contenuto dell'incarico

(1) **Tipo e scopo del trattamento previsto dei dati**

- Finalità 1 - Inquadrare il modello aziendale del committente / offerta del servizio:

  Soluzione tecnica per poter inquadrare il modello aziendale del committente; questa comprende sia la realizzazione di esperienze sulla piattaforma bookingkit sia un inquadramento tecnico delle condizioni, del procedimento desiderato di prenotazione, del processo di comunicazione con i clienti finali e dei processi aziendali aggiuntivi del titolare del trattamento

- Zweck 2 - Verwaltung des Treuhandkontos:

  Verwaltung des Treuhandkontos des Auftraggebers, um Zahlungen für ihn zu akzeptieren und Auszahlungen zu verarbeiten;

- Zweck 3 - Übermittlung von Informationen zu Diensten des Auftragnehmers:

  Informationen über Änderungen der Dienste des Auftragnehmers übermitteln, die dem Auftraggeber dazu dienen, sein Geschäft effizienter/effektiver abzuwickeln.

- Zweck 4 - Hilfestellung Service-Team:

  Direkte Hilfestellung für die Dienste des Auftragnehmers durch sein Serviceteam auf Anfrage des Auftraggebers oder proaktiv sollte Handlungsbedarf durch den Auftragnehmer festgestellt oder empfohlen sein

- Zweck 5 – Ermöglichung der Vermarktung über Partner

  Technische Lösung, um dem Auftraggeber zu ermöglichen, seine Angebote mithilfe ausgewählter Partnerunternehmen zu vermarkten. Hierzu kann der Auftraggeber die Weitergabe seiner Kontaktdaten und die Daten der von ihm angebotenen Erlebnisse an entsprechende Partner veranlassen, sofern er mit diesen zusammenarbeiten möchte, so dass der Partner mit dem Anbieter für eine Vertragsanbahnung in Kontakt tritt.

- Zweck 6 – Speicherung von Identitätsnachweisen

  Zum Zwecke des vertragsgemäßen Anlegens von Treuhandkonten und zur Ermöglichung der Zusammenarbeit mit Zahlungsanbietern im Rahmen der Vertragserfüllung in Anlehnung an § 11 Geldwäschegesetz sowie zum Zwecke des Nachweises von

- Finalità 2 - Gestione del conto fiduciario:

  Gestione del conto fiduciario del committente, per accettare i pagamenti per lui e per elaborare i pagamenti;

- Finalità 3 - Trasmissione di informazioni sui servizi del fornitore:

  Trasmettere informazioni sulle modifiche ai servizi del Fornitore che servono al Committente per svolgere le sue attività commerciali in modo più efficiente/efficace.

- Finalità 4 - Predisposizione del team di assistenza:

  Predisposizione diretta dei servizi del Fornitore tramite team di assistenza su richiesta del Committente oppure proattivamente, qualora sia stabilita o consigliata la necessità d'intervento da parte del Fornitore

- Finalità 5 - Possibilità di commercializzazione tramite partner

  Soluzione tecnica per consentire al Committente di commercializzare le sue offerte per mezzo di aziende partner selezionate.

  A tal fine, il Committente può assegnare a partner corrispondenti l'inoltro dei suoi dati di contatto e i dati dei servizi da lui offerti, purché desideri collaborare con loro, di modo che il partner entri in contatto con il fornitore per un principio di contratto.

- Scopo 6: Salvataggio dei documenti di riconoscimento

  Al fine di realizzare, come da contratto, dei conti fiduciari e di consentire la collaborazione con fornitori di pagamento nel quadro dell'adempimento contrattuale in riferimento all'art. 11 della legge sul riciclaggio del danaro e al fine di comprovare controlli su elenchi di sanzioni realizzati ad alti livelli.

Prüfungen von hoheitlich erstellten Sanktionslisten.

(2) **Art der Daten -** Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Angaben zur Person:
  - Name
  - Anschrift
  - Geburtsdatum
  - Email Adresse
  - Telefonnnummer
  - Ggf. IBAN
  - Ggf. BIC
  - Ggf. Firmenname
  - Ggf. Steuernummer
  - Ggf. Kopie des Lichtbildausweises
- Online-bezogene Daten:
  - Cookie/ Sitzungsidentifikationsnummer
  - IP Adresse (zur Identifikation bei Vertragsabschluss)
  - Zeitstempel
  - Login-Daten
- Kundendaten:
  - Name
  - E-Mail Adresse
  - Zahlungsart

(3) **Kategorien betroffener Personen** - Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Angestellte
- Auszubildende
- Gewerbliche Mitarbeiter
- Interessenten
- Kunden
- Mitarbeiter
- Praktikanten
- User

(2) **Tipi di dati -** Oggetto del trattamento dei dati personali sono i seguenti tipi/categorie:

- Informazioni sulla persona:
  - Nome
  - Recapito
  - Data di nascita
  - Indirizzo e-mail
  - Numero di telefono
  - Eventuale IBAN
  - Eventuale BIC
  - Eventuale nome dell'azienda
  - Eventuale codice fiscale
  - Eventuale copia di una fototessera
- Dati identificativi online:
  - Cookie/Numero di identificazione della sessione
  - Indirizzo IP (per l'identificazione alla stipulazione del contratto)
  - Marcatura temporale
  - Dati di accesso
- Dati del cliente:
  - Nome
  - Indirizzo e-mail
  - Metodo di pagamento

(3) **Categorie di persone interessate -** Le categorie di persone interessate dal trattamento comprendono:

- Impiegati
- Apprendisti
- Operai
- Parti interessate
- Clienti
- Collaboratori
- Tirocinanti
- Utenti

3 Technisch-organisatorische Maßnahmen

3 Provvedimenti tecnico-organizzativi

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten

(1) Il Fornitore deve documentare l'implementazione dei provvedimenti tecnici e organizzativi necessari e predisposti nella fase introduttiva dell'assegnazione del trattamento prima dell'inizio del trattamento, in particolare per ciò che riguarda l'esecuzione concreta dell'incarico nonché trasmetterli al Committente per un controllo. Una volta accettati dal Committente, i provvedimenti documentati diventano principio fondamentale dell'incarico. Se il controllo/un audit del Committente rivela l'esigenza di adeguamento, questo dovrà essere implementato in modo consensuale.

(2) Il Fornitore deve garantire la sicurezza ai sensi dell'art. 28, comma 3, lett. c, 32 RGPD in particolare in combinazione con l'art. 5, comma 1, comma 2 RGPD. Nel complesso, con provvedimenti s'intendono misure relative alla sicurezza dei dati e alla garanzia di un livello di protezione idoneo al rischio sul piano della riservatezza, dell'integrità, della disponibilità e della tollerabilità dei sistemi. In questo contesto si devono considerare lo stato dell'arte e i costi di attuazione e la natura, l'ambito di applicazione e le finalità del trattamento, nonché la probabilità e la gravità del rischio per i diritti e le libertà delle persone fisiche ai sensi dell'art. 32, comma 1 RGPD [specifiche indicate nell'Allegato 1].

(3) I provvedimenti tecnici e organizzativi sono soggetti al progresso tecnologico. Se possibile per il Fornitore, dovranno essere implementati provvedimenti adeguati alternativi. In questo contesto, il livello di sicurezza non deve essere inferiore a quello prestabilito dai provvedimenti. Documentare eventuali modifiche sostanziali.

werden. Wesentliche Änderungen sind zu dokumentieren.

4

Berichtigung, Einschränkung und Löschung von Daten

(1) 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. Die Weisung muss schriftlich erfolgen über die Emailadresse datenschutz@bookingkit.de. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

5

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

4

Rettifica, limitazione e cancellazione dei dati

(1) Il Fornitore deve rettificare, cancellare (o limitare il trattamento) dei dati trattati nell'ambito dell'incarico, non di propria iniziativa bensì in seguito a un'istruzione documentata del Committente. L'istruzione deve essere comunicata in forma scritta contattando l'indirizzo e-mail dataprotection@bookingkit.de. Se una persona interessata si rivolge, a tal proposito, direttamente al Fornitore, il Fornitore inoltrerà immediatamente questa richiesta al Committente.

(2) Se previsto dalla fornitura del servizio, il Fornitore deve garantire immediatamente il concetto di cancellazione, il diritto all'oblio, alla rettifica, alla portabilità dei dati e all'informazione su istruzione documentata del Committente.

5

Garanzia di qualità e altri obblighi del Fornitore

Il fornitore ha, in aggiunta all'osservanza delle disposizioni del presente incarico, obblighi legali ai sensi degli art. da 28 a 33 RGPD, garantendo in particolare il rispetto delle seguenti indicazioni:

a. Nomina scritta di un responsabile della protezione dei dati che esercita la sua attività ai sensi degli art. 38 e 39 RGPD.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer die ePrivacy GmbH vertreten durch Prof. Dr. Christoph Bauer, Große Bleichen 21, 20354 Hamburg, telefonisch zu erreichen unter +49 (0) 40 609451810 und per E-Mail über datenschutz@bookingkit.de bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

In qualità di responsabile della protezione dei dati è nominata l'azienda ePrivacy GmbH rappresentata dal Prof. Dr. Christoph Bauer, Große Bleichen 21, 20354 Hamburg, raggiungibile telefonicamente al numero +49 (0) 40 609451810 e via e-mail all'indirizzo dataprotection@bookingkit.de. La sostituzione del responsabile della protezione dei dati deve essere comunicata immediatamente al Committente.

b. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die während des Auftrags und nach dessen Beendigung auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b. Garanzia di riservatezza ai sensi degli art. 28, comma 3, f. 2, lett. b, 29, 32, comma 4 RGPD. Per l'esecuzione dei lavori, il Fornitore, per la durata del contratto e dopo il suo completamento,, impiega esclusivamente dipendenti che s'impegnano a garantire la riservatezza e con conoscenza consolidata delle disposizioni pertinenti la protezione dei dati. Il Fornitore e ogni persona subordinata del Fornitore, che ha accesso a dati personali, devono trattare questi dati esclusivamente in conformità con l'istruzione del Committente, inclusi i poteri previsti dal presente contratto salvo che siano vincolati al trattamento per legge.

c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

c. Implementazione e osservanza di tutti i provvedimenti tecnici e organizzativi necessari per questo incarico ai sensi degli art. 28, comma 3, f. 2, lett. c, 32 RGPD [specifiche indicate nell'Allegato 1].

d. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d. Il Committente e il Fornitore collaborano su richiesta dell'autorità di controllo per l'adempimento delle proprie attività.

e. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen

e. L'informazione tempestiva del Committente sulla gestione dei controlli e sui provvedimenti dell'autorità di controllo, se si riferiscono a questo incarico. Ciò si applica, anche se un'autorità

eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f. 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.

g. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

competente indaga presso il Fornitore, nel quadro di disposizioni repressive relative al trattamento di dati personali, per la responsabilità del trattamento.

f. Se il Committente, da parte sua, è esposto a un controllo dell'autorità di controllo, a disposizioni repressive, alla richiesta di responsabilità di una persona interessata oppure un terzo o a un'altra richiesta associata alla responsabilità del trattamento presso il Fornitore, il Fornitore dovrà sostenerlo con le migliori risorse.

g. Il Fornitore controlla regolarmente i processi interni nonché i provvedimenti tecnici e organizzativi al fine di garantire che il trattamento abbia luogo nel suo ambito di responsabilità in armonia con i requisiti del diritto vigente sulla protezione dei dati e che sia garantita la protezione dei diritti della persona interessata.

h. Dimostrabilità dei provvedimenti tecnici e organizzativi interessati nei confronti del Committente nel quadro dei suoi poteri di controllo secondo la clausola 7 del presente contratto.

6

Unterauftragsverhältnisse

(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 Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie

6

Rapporti contrattuali delegati

(1) Con rapporti contrattuali delegati s'intendono, ai sensi di questo regolamento, quei servizi che si riferiscono immediatamente alla prestazione del servizio principale. Non vi rientrano i servizi secondari di cui si avvale il Fornitore, ad es. servizi di telecomunicazioni, servizi postali/trasporto, manutenzione e servizi agli utenti oppure lo smaltimento di supporti dati nonché

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.

eventuali provvedimenti per garantire la riservatezza, la disponibilità, l'integrità e la tollerabilità di hardware e software di strutture di trattamento dei dati. Tuttavia, il Fornitore ha l'obbligo di stipulare accordi contrattuali adeguati e conformi alla legge, e intraprendere provvedimenti di controllo a garanzia della protezione dei dati e della sicurezza dei dati del Committente anche per i servizi secondari esternalizzati.

(2) Die Auslagerung auf Unterauftragnehmer und der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt, wobei die Anzeige auch durch Vorab-Aktualisierung des Anhangs 2 dieser Vereinbarung geschehen kann, welche durch den Auftraggeber in regelmäßigen Abständen geprüft wird, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben, und
- die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) L'esternalizzazione a fornitori delegati e la sostituzione dell'attuale fornitore subordinato sono ammesse, se:

- l Fornitore informa il Cliente di qualsiasi intenzione di esternalizzare a subappaltatori con un adeguato periodo di preavviso in forma scritta o in forma testuale; tale indicazione può avvenire anche attraverso l'aggiornamento preliminare dell'Appendice 2 del presente contratto, che viene controllato a intervalli regolari dal Cliente, il quale ha la possibilità di opporsi a tali modifiche e si soddisfano i particolari prerequisiti degli art. 44 ss. RGPD.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(3) La trasmissione dei dati personali del Committente al fornitore delegato e la sua prima attività devono, prima di tutto, essere dotate della predisposizione di tutti i prerequisiti per una subdelega.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn

(4) Se il fornitore delegato presta il servizio concordato al di fuori della UE/dello SEE, il Fornitore assicura la liceità giuridica con provvedimenti idonei. Lo stesso dicasi se devono

Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch den Unterauftragnehmern aufzuerlegen.

essere impiegati fornitori di servizi ai sensi del comma 1 frase 2.

(5) Tutti i regolamenti contrattuali nella catena contrattuale devono essere imposti al fornitore delegato.

7

Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter,

7

Diritti di controllo del Committente

(1) Il Committente ha il diritto, in consultazione con il Fornitore, di eseguire controlli oppure di lasciarli eseguire, nel singolo caso, da un ente di controllo da nominare. Attraverso controlli a campione che, normalmente, sono comunicati per tempo, egli ha il diritto di convincersi dell'osservanza del presente contratto da parte del Fornitore nell'esercizio delle sue attività commerciali.

(2) Il Fornitore si assicura che il Committente può convincersi dell'osservanza degli obblighi del fornitore ai sensi dell'art. 28 RGPD. Il Fornitore s'impegna a comunicare al Committente, su richiesta, le informazioni necessarie e, in particolare, a comprovare l'implementazione dei provvedimenti tecnici e organizzativi.

(3) La prova di tali provvedimenti, che interessano non soltanto l'incarico concreto, può avere luogo tramite

- l'osservanza di codici di condotta approvati ai sensi dell'art. 40 RGPD;
- la certificazione nel rispetto di un procedimento approvato di certificazione ai sensi dell'art. 42 RGPD;
- attestati attuali, relazioni o estratti di relazioni di enti di verifica indipendenti (ad es. revisori contabili, revisione, responsabile

IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

della protezione dei dati, reparti di sicurezza IT, auditor per la protezione dei dati, auditor di qualità);

- una certificazione idonea tramite audit sulla sicurezza IT o audit sulla protezione dei dati (ad es. la protezione fondamentale BSI).

(4) Per consentire i controlli da parte del Committente, il Fornitore può richiedere una compensazione.

8

Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers

8

Comunicazione in caso di violazioni del Fornitore

(1) Il Fornitore supporta il Committente nell'osservanza degli obblighi indicati agli articoli da 32 a 36 RGPD per la sicurezza dei dati personali, obblighi di notifica in caso di violazioni dei dati, valutazioni dell'impatto della protezione dei dati e previe consultazioni. Questi comprendono, tra gli altri,

a. la garanzia di un livello di protezione idoneo mediante provvedimenti tecnici e organizzativi che prendono in considerazione le circostanze e le finalità del trattamento nonché la probabilità e la gravità previste di una possibile violazione di diritto per via di lacune nella sicurezza e che consentono una decisione immediata di eventi pertinenti alla violazione
b. l'obbligo, di segnalare tempestivamente al Committente violazioni di dati personali
c. l'obbligo di supportare il Committente nel quadro del suo obbligo d'informazione nei confronti dell'interessato e di mettergli immediatamente a disposizione tutte le informazioni pertinenti ivi associate
d. il sostegno del Committente per la rispettiva valutazione dell'impatto sulla protezione dei dati
e. il sostegno del Committente nel quadro delle previe consultazioni con l'autorità di controllo

(2) Per i servizi di supporto, che non sono contenuti nella descrizione del servizio oppure che non riconducono a un comportamento erroneo del

zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9

Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10

Löschung und Rückgabe von personenbezogenen Daten

(1) 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte

Fornitore, il Fornitore può richiedere una compensazione.

9

Autorità del Committente

(1) Il Committente conferma le istruzioni orali immediatamente (almeno in forma scritta).

(2) Il Fornitore deve informare immediatamente il Committente se è dell'opinione che un'istruzione viola le disposizioni sulla protezione dei dati. Il Fornitore è autorizzato ad attuare l'esecuzione dell'istruzione corrispondente se è stata confermata o modificata dal Committente.

10

Cancellazione e restituzione dei dati personali

(1) Copie o duplicati dei dati non sono realizzati senza mettere prima a conoscenza il Committente. Questa condizione esclude copie di sicurezza, se necessarie per garantire un trattamento conforme dei dati, nonché dati che sono necessari nell'ambito dell'osservanza degli obblighi di conservazione stabiliti per legge.

(2) Al termine dei lavori concordati per contratto oppure in precedenza, su richiesta del Committente - al più tardi con il termine dell'accordo di fornitura - il Fornitore deve cedere al Committente tutti i documenti che sono giunti in suo possesso, esiti inerenti al trattamento e all'utilizzo e

Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ausgenommen sind Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, welche der Auftragnehmer aufgrund rechtlicher Bestimmungen aufzubewahren hat.

banche dati associati al rapporto d'incarico, oppure distruggerli previo accordo e nel rispetto del diritto per la protezione dei dati. La stessa condizione si applica al materiale di prova e di scarto. Il protocollo per la cancellazione deve essere esibito su richiesta. Fanno eccezione i documenti, gli esiti inerenti al trattamento e all'utilizzo nonché banche dati associati al rapporto d'incarico che il Fornitore deve conservare nel rispetto delle disposizioni giuridiche.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(3) Documentazioni che servono a comprovare il trattamento dei dati conforme all'incarico e alle disposizioni devono essere conservate dal Fornitore nel rispetto dei termini di conservazione oltre la fine del contratto. A suo discarico, al termine del contratto può cederli al Committente.

ANLAGE 1
Technisch-organisatorische Maßnahmen

1

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

a. Zutrittskontrolle

- Der Auftragnehmer stellt anhand von elektronischen Schlüsseln sicher, dass nur autorisierte Personen Zutritt zu ihren Räumlichkeiten haben. Diese können individuell gesperrt werden.
- Außerdem ist das Bürogelände des Auftragnehmers 24 Stunden täglich von einem Wachdienst geschützt, welcher regelmäßig Rundgänge durchführt.
- Es ist ein Alarmsystem installiert, welches mit einem Schließmechanismus für die Türen gekoppelt ist.
- Die Tür des Serverraums ist mit einem Schlüssel gesichert, welcher nur dem zuständigen Personal zur Verfügung steht.
- Mitarbeitern im Homeoffice ist es untersagt, außerhalb des Bürogeländes betriebliche Unterlagen auf Papier oder portablen Datenträgern zu nutzen. Daten sind ausschließlich über die zentrale Datenverwaltung zu nutzen.

b. Zugangskontrolle

- Der Auftragnehmer gewährt Mitarbeitern nur auf die Systeme Zugriff, welche er für die Ausführung seiner konkreten Aufgaben benötigt.

ALLEGATO 1
Provvedimenti tecnico-organizzativi

1

Riservatezza (art. da 32, comma 1, lett. b RGPD)

a. Controllo dell'accesso

- Con l'ausilio di chiavi elettroniche, il Fornitore si assicura che soltanto le persone autorizzate hanno accesso ai suoi ambienti. Questi ultimi possono essere bloccati singolarmente.
- Inoltre, l'area dell'ufficio del Fornitore deve essere protetta 24 ore su 24 da un vigilante che compie regolarmente delle ronde.
- È installato un sistema di allarme abbinato a un meccanismo di chiusura delle porte.
- La porta del locale dei server è protetta con una chiave disponibile esclusivamente al personale competente.
- Ai dipendenti dell'ufficio di casa è vietato utilizzare documenti aziendali su supporto cartaceo o portatile all'esterno dei locali dell'ufficio. I dati possono essere utilizzati solo tramite la gestione centrale dei dati.

b. Controllo dell'accesso

- Il Fornitore garantisce l'accesso ai collaboratori soltanto ai sistemi necessari al fine di svolgere le mansioni concrete.

- Den Zugang zu den eigenen Systemen regelt der Auftragnehmer über sichere personalisierte Passwörter und Passwortverfahren. Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account geknüpft. Außerdem verfügen alle Mitarbeiter des Auftragnehmers über ein Passwortmanagementsystem, welches im Bedarfsfall zufällige Passwörter für sensible Systeme festlegt.
- Passwörter des Auftragnehmers unterliegen Mindestanforderungen an Sicherheitsbestimmungen.
- Alle Datenträger und Laptops sind verschlüsselt.
- Alle Windows Laptops nutzen die Full Disk Hardware Encryption der verbauten SSDs. Alle Macbooks nutzen die integrierte Filevault Encryption von MacOS.
- Alle Computer verfügen über Virenscanner, welche täglich geupdated werden.

c. Zugriffskontrolle

- Zugangsberechtigte können nur auf Daten zugreifen, die in ihrem individuellen Berechtigungsprofil eingerichtet sind.
- Zum Erstellen und Ändern von Berechtigungsprofilen gibt es strenge Regelungen und Verfahren, welche die Genehmigung durch die Geschäftsführung einschließen.
- Das Sperren bzw. Abmelden beim Verlassen des Arbeitsplatzes ist schriftlich angeordnet und wird praktiziert.
- Alle Server und Services des Auftragnehmers werden kontinuierlich überwacht.

- L'accesso ai propri sistemi è regolamentato dal Fornitore tramite password personalizzate sicure e procedimenti con password. Le autorizzazioni sono associate al riconoscimento individuale dell'utente e a un account. Inoltre, tutti i collaboratori del Fornitore dispongono di un sistema di gestione delle password che, all'occorrenza, stabilisce le password necessarie per i sistemi sensibili.
- Le password del Fornitore sono soggette ai requisiti minimi delle disposizioni di sicurezza.
- Tutti i supporti dati e i laptop sono codificati.
- Tutti i laptop Windows utilizzano una tecnologia Full Disk Hardware Encryption dell'SSD integrato. Tutti i Macbook utilizzano la tecnologia Filevault Encryption di MacOS.
- Tutti i computer dispongono di scanner per virus, aggiornati quotidianamente.

c. Controllo dell'accesso

- Le persone con accesso autorizzato possono accedere soltanto ai dati configurati nel profilo di autorizzazione individuale.
- Per realizzare e modificare i profili di autorizzazione sono previsti regolamenti e procedimenti rigidi che comprendono l'autorizzazione da parte dell'amministrazione aziendale.
- Il blocco e/o l'uscita quando si lascia la propria postazione di lavoro sono stabiliti per iscritto e messi in atto.
- Tutti i server e i servizi del Fornitore sono monitorati costantemente.

d. Trennungskontrolle

- Berechtigungskonzepte verhindern die ungeplante Verwendung sensibler Daten. Der Zugriff auf die Daten selbst ist zudem dadurch eingeschränkt, dass die Mitarbeiter Services (Applikationen) verwenden, welche den Zugriff steuern und kein Beschreiben der Daten zulassen.
- Alle Kundendaten werden in der selben Datenbank verwaltet, da es systembedingt nicht möglich ist diese auf Datenbankebene zu trennen. Da ohnehin ausschließlich über entsprechende Software auf die Daten zugegriffen werden darf, wird Trennung über ein Rollenkonzept in der Software sichergestellt.
  Ausnahmen gelten für Developer und das Customer Success Team, die zur Fehlerbehebung direkt auf die Datenbank zugreifen dürfen. Dieser Zugriff erfolgt ausschließlich lesend, so dass keine Daten am Rollenkonzept vorbei verändert werden können.
- Es gibt ein abgetrenntes WLAN für Gäste.
- Es erfolgt eine Trennung von Test- und Produktivsystemen. Sollten Softwareneuerungen der Trennungskontrolle nicht genügen, werden diese im Testsystem aufgedeckt und nicht in das Produktivsystem übernommen.

e. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Daten für interne Auswertungen zu statistischen Zwecken zur Produktivitätssteigerung werden vor der Verarbeitung anonymisiert indem die IP Adressen gekürzt bzw. zufällig verändert werden.

d. Controlli della suddivisione

- I concetti di autorizzazione impediscono l'impiego imprevisto di dati sensibili. L'accesso stesso ai dati stessi è, a tal fine, limitato dal fatto che i collaboratori usino servizi (applicazioni) che controllano l'accesso e non concedano la descrizione dei dati.
- Tutti i dati dei clienti sono gestiti nella stessa banca dati, dal momento che non è possibile suddividerli su livelli della banca dati. Dal momento che, in ogni caso, è possibile accedere ai dati soltanto con il software corrispondente, la suddivisione è garantita da un concetto di ruoli nel software. Le eccezioni sono applicabili ai developer e al Customer Success Team che possono accedere direttamente alla banca dati per una ricerca guasti. Questo accesso ha luogo soltanto in modalità di lettura, pertanto nessun dato può essere modificato per ciò che riguarda il concetto di ruoli.
- Per gli ospiti è predisposta una rete WLAN a parte.
- È in atto la suddivisione tra sistemi di prova e sistemi di produzione. Qualora gli aggiornamenti software del controllo sulla divisione non fossero sufficienti, questi sono coperti nel sistema di prova e non acquisiti nel sistema di produzione.

e. Pseudonimizzazione (art. 32, comma 1, lett. a RGPD, art. 25, comma 1 RGPD)

- I dati per le valutazioni interne per finalità statistiche volte all'incremento della produttività sono anonimizzati prima del trattamento, con conseguente abbreviazione degli indirizzi IP ed eventuale modifica.

- Insbesondere im Bereich des Onlinemarketings wird ausschließlich mit pseudonymen Online-Identifiern und -Profilen gearbeitet. Diese werden mittels des sogenannten hashings pseudonymisiert

- In particolare, nel settore del marketing online si lavora esclusivamente con identificativi online e profili online pseudonimizzati. Questi sono pseudonimizzati per mezzo del cosiddetto hashing

2

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

a. Weitergabekontrolle

- Alle Transportwege sind SSL-verschlüsselt.
- Das Rechtemanagement für die Datenauslesung des Auftraggebers liegen beim Auftraggeber.
- Der Verkehr zwischen den Systemen ist über SSL/TLS verschlüsselt.
- Das Frontend verfügt über eine Https-Verschlüsselung.
- Der Zugang zu den Systemen von außen ist über open VPN verschlüsselt. Mitarbeiter mit VPN Zugang müssen sich über Benutzername/Passwort und ein Zertifikat authentifizieren.
- Hardwarekomponenten oder Dokumente werden so vernichtet, dass eine Wiederherstellung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.
- Die Datenübertragung zwischen Clients und Servern erfolgt verschlüsselt.
- Für die Anfertigung von Kopien gibt es eindeutige Regelungen und Verfahrensweisen.
- Es existieren mehrere Firewalls.
- Auf sämtlichen Arbeitsstationen existieren Firewalls, welche ständig

2

Integrità (art. 32, comma 1, lett. b RGPD)

a. Controllo dell'inoltro

- Tutte le vie di trasporto sono con codifica SSL.
- La gestione del diritto per la lettura dei dati del Committente è di competenza del Committente.
- Il traffico tra i sistemi è codificato tramite SSL/TLS.
- Il frontend dispone di una codifica https.
- L'accesso ai sistemi dall'esterno è codificato tramite VPN. I collaboratori con accesso VPN devono autenticarsi tramite nome utente/password e un certificato.
- I componenti hardware oppure i documenti sono distrutti in modo che non sia possibile un ripristino oppure che questo sia possibile soltanto con un dispendio elevato di energie.
- La trasmissione dei dati tra client e server ha luogo con codifica.
- Per la realizzazione di copie sono in atto regolamenti e procedimenti univoci.
- Sono disponibili diversi firewall.
- Presso tutte le postazioni di lavoro sono disponibili firewall attivati

aktiviert sind und durch den Nutzer nicht deaktivierbar sind.

b. Eingabekontrolle

- Die Mitarbeiter außerhalb der Entwicklungsabteilung des Auftragnehmers arbeiten nicht direkt auf Datenbankebene, sondern nutzen Applikationen, um auf die Daten zuzugreifen.
- Datenbankstrukturänderungen werden detailliert im Projektmanagementtool JIRA protokolliert. Die Protokolle werden revisionssicher 12 Monate lang aufbewahrt. Die Eingabe, Änderung und Löschung von Daten kann dabei anhand von individuellen Benutzernamen nachvollzogen werden.
- IT-Mitarbeiter verwenden einen gemeinsamen Login für die Datenbanken, da es wenige Mitarbeiter sind, die räumlich beieinander sitzen. Durch Absprachen und Sichtkontrollen wird die Arbeit an den Datenbanken zusätzlich überwacht.

costantemente e non disattivabili dall'utente.

b. Controllo dell'immissione

- I collaboratori al di fuori del reparto di sviluppo del Fornitore non lavorano direttamente a livello della banca dati, bensì impiegano le applicazioni per accedere ai dati.
- Modifiche alla struttura della banca dati sono protocollate in dettaglio nel tool di gestione dei progetti JIRA. I protocolli sono conservati per 12 mesi a scopo di revisione. L'immissione, la modifica e la cancellazione dei dati possono essere eseguite con il nome utente personale.
- I collaboratori IT impiegano il login comune per le banche dati, dal momento che sono in pochi e siedono in ambienti limitrofi. Colloqui e controlli visivi consentono di monitorare il lavoro sulle banche dati.

3

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

Verfügbarkeitskontrolle

- Der Auftragnehmer erstellt täglich ein weiteres Gesamt-Backup, welches für 7 Tage gespeichert wird. Auf diese Backups kann zurückgegriffen werden, sollten andere Verfügbarkeitsmaßnahmen versagen. Es handelt sich hierbei um ein Gesamtbackup, welches nicht zur Wiederherstellung einzelner Daten herangezogen werden kann, sondern lediglich das komplette System wiederherstellt.

§ 3

Disponibilità e tollerabilità (art. 32, comma 1, lett. b RGPD)

Controllo della disponibilità

- Il Fornitore redige quotidianamente un back-up complessivo che viene conservato per 7 giorni. È possibile accedere a questi backup, qualora altri provvedimenti sulla disponibilità dovessero fallire. In questo caso, si tratta di un back-up complessivo che non può essere impiegato per il ripristino di singoli dati, bensì soltanto per ripristinare l'intero sistema.

- Aus diesen Backups kann jederzeit im Falle eines Notfalls das System wiederhergestellt werden.
- Es existiert ein Notfallplan, aus welchem hervor geht, welche Schritte wann eingeleitet werden müssen und welche Personen und Stellen zu welchem Zeitpunkt und welchem Zweck informiert werden müssen.
- Die einzelnen Arbeitsstationen beim Auftragnehmer sind über täglich geupdatete Virenscans geschützt, die Datenträger sind verschlüsselt.
- Unsere Server und Backup-Systeme stehen in den Rechenzentren von Amazon Web Services welche umfassend für die Betriebskontinuität geschützt sind. Details dazu können sie hier nachlesen: https://aws.amazon.com/de/compliance/data-center/controls/
- Hochverfügbare Systeme werden parallel in mehreren Rechenzentren redundant betrieben.
- Die Überlastung von Servern ist durch eine sogenannte autoscaling group ausgeschlossen. Steigt die Last auf die Server werden automatisiert weitere Server hinzu geschaltet, um eine Überlastung zu verhindern.
- Sämtliche Betriebsparameter werden permanent überwacht.

- Il sistema può essere ripristinato da questi backup in qualsiasi momento si verifichi una situazione di emergenza.
- È in atto un piano di emergenza che indica i diversi passi da intraprendere e quali persone e sedi devono essere informate per quale finalità.
- Le singole postazioni di lavoro presso il Fornitore sono protette con scansioni antivirus aggiornate quotidianamente e i supporti dati sono codificati.
- I nostri server e sistemi di backup si trovano nei centri di calcolo di Amazon Web Services che sono protetti in modo esauriente per la continuità aziendale. I dettagli sono disponibili qui: https://aws.amazon.com/it/compliance/data-center/controls/?nc1=h_ls
- Sistemi ad alta disponibilità sono in esercizio parallelo in diversi centri di calcolo.
- Il sovraccarico di server è escluso grazie al cosiddetto autoscaling group. Se il carico dei server aumenta, altri server sono attivati automaticamente per impedire il sovraccarico.
- Tutti i parametri di funzionamento sono monitorati costantemente.

4

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

4

Procedura per il controllo, la valutazione e la valutazione regolari (art. 32 comma 1 let. d RGPD; art. 25 comma 1 RGPD)

a. Datenschutz Management

- Der Auftragnehmer überprüft regelmäßig ihr Datenschutz-Management unter Einbeziehung des betrieblich bestellten Datenschutzbeauftragten.
- Sämtliche Mitarbeiter werden regelmäßig zum Thema Datenschutz geschult. Außerdem werden alle Mitarbeiter auf das Datengeheimnis verpflichtet. Mitarbeiter im Homeoffice werden auf die besonderen Regeln gesondert belehrt.

b. Incident Response Management

- Im Falle einer Datenpanne greift ein umfassendes Regelwerk zu einzuleitenden Prozessen und Kommunikationsschritten.
- Für die gegebenenfalls zu erfolgende Information von Aufsichtsbehörden sind die verantwortlichen Mitarbeiter geschult, so dass einer Information innerhalb von 72 Stunden nichts im Wege steht.

c. Datenschutzfreundliche Voreinstellungen

- Bei der Entwicklung jeder Technologie oder jedes neuen Produktes wird von vornherein ein Privacy by Design-Ansatz verfolgt. Es wird von vornherein das Ziel verfolgt, die Menge der zu erhebenden Daten zu minimieren und den Umfang der Datenverarbeitung zu reduzieren
- Soweit möglich werden Daten nur pseudonymisiert weiterverarbeitet. Datenschutzerklärungen, welche leicht zugänglich sind und sämtliche Datenprozesse ausführlich beschreiben, sorgen für Transparenz.

d. Auftragskontrolle

- Sämtliche Auftragnehmer sind unter Sorgfaltsgesichtspunkten ausgewählt.

a. Gestione della protezione dei dati

- Il Fornitore controlla regolarmente la sua gestione della protezione dei dati coinvolgendo il responsabile della protezione dei dati nominato dall'azienda.
- Tutti i collaboratori sono regolarmente formati in materia di protezione dei dati. Inoltre, tutti i collaboratori sono vincolati al segreto sui dati.
  I dipendenti nell'ufficio di casa sono istruiti separatamente sulle regole speciali.

b. Incident Response Management

- Nel caso di una violazione dei dati, un quadro legislativo esteso innesca processi e fasi di comunicazione.
- Per le informazioni da seguire, all'occorrenza, dalle autorità di controllo, i collaboratori responsabili ricevono una formazione tale che l'informazione sia veicolata entro 72 ore.

c. Disposizioni a favore della protezione dei dati

- Per lo sviluppo di ogni tecnologia o ogni nuovo prodotto è previsto, sin dal principio, un approccio del tipo Privacy by Design. Sin dal principio si persegue l'obiettivo di ridurre al minimo la quantità di dati da raccogliere e ridurre la portata del trattamento dei dati
- Se possibile, i dati sono trattati in forma soltanto pseudonimizzata. Dichiarazioni sulla protezione dei dati, di facile accesso e che descrivono tutti i processi sui dati, garantiscono trasparenza.

d. Controlli dell'incarico

- Tutti i fornitori sono selezionati con la massima attenzione.

- Mit sämtlichen Auftragnehmers werden Auftragsverarbeitungsverträge abgeschlossen und technische und organisatorische Maßnahmen werden regelmäßig überprüft.
- Kontrollrechte werden mit Auftragnehmern vertraglich vereinbart.

- Con tutti i fornitori sono stipulati accordi di fornitura e i provvedimenti tecnici e organizzativi sono verificati regolarmente.
- I diritti al controllo sono concordati contrattualmente con i fornitori.

ANLAGE 2
Unterauftrags-verhältnisse

Präambel

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 Auftragnehmer 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.

1

Bestehende Unterauftragsverhältnisse

Eine Liste von bestehenden Unterauftragsverhältnisse ist unter folgendem Link abrufbar: https://bookingkit.net/legaldocuments-dpa-list/

2

Bestehende Unterauftrags-verhältnisse mit Unternehmen aus Drittländern

ALLEGATO 2
Rapporti contrattuali subordinati

Premessa

Con rapporti contrattuali delegati s'intendono, ai sensi di questo regolamento, quei servizi che si riferiscono immediatamente alla prestazione del servizio principale. Non vi rientrano i servizi secondari di cui si avvale il Fornitore, ad es. servizi di telecomunicazioni, servizi postali/trasporto, manutenzione e servizi agli utenti oppure lo smaltimento di supporti dati nonché eventuali provvedimenti per garantire la riservatezza, la disponibilità, l'integrità e la tollerabilità di hardware e software di strutture di trattamento dei dati.

1

Accordi di subappalto

La lista degli accordi di subappalto è disponibile al link seguente: https://bookingkit.net/legaldocuments-dpa-list/

2

Accordi di subappalato in essere con aziende da paesi terzi

Eine Liste von bestehenden Unterauftragsverhältnisse mit Unternehmen aus Drittländern ist unter folgendem Link abrufbar: https://bookingkit.net/legaldocuments-dpa-list-2/

La lista degli accordi di subappalto con aziende terze è disponibile al seguente link: https://bookingkit.net/legaldocuments-dpa-list-2/

bookingkit

Vertrag zur Auftragsverarbeitung

Contrat relatif à la sous-traitance en vertu

VEREINBARUNG zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

- Verantwortlicher, nachstehend Auftraggeber genannt –
und

ACCORD relatif à la sous-traitance en vertu de l'article 28 du RGPD

entre

- Responsable, ci-après désignée « le client » -
et

bookingkit GmbH
vertreten durch / *représentée par* Christoph Kruse et Lukas C. C. Hempel
Sonnenallee 223
D-12059 Berlin

- Auftragsverarbeiter, nachstehend Auftragnehmer genannt -

- Sous-traitant, ci-après désignée « le fournisseur » -

Note importante: seule la version originale en allemand de ce contrat prévault.
La traduction francais vous est fournie à titre d'information.

Definitionen

Die nachfolgend aufgeführten Begriffe haben für diesen Vertrag die ihnen daneben zugeordnete Bedeutung, soweit sich aus dem Kontext nicht ausdrücklich etwas anderes ergibt:

"bookingkit Plattform":
Die Gesamtheit der Dienste des Auftragnehmers

„Drittländer":
Länder außerhalb der EU/ des EWR

Définitions

Dans le cadre de ce contrat, les termes ci-dessous ont la signification suivante, dans la mesure où ils sont utilisés dans ce contexte précis :

« Plateforme bookingkit » :
L'ensemble des services mis à disposition par le fournisseur

« Pays tiers » :
Tout pays en dehors de l'UE/de l'EEE

1

Gegenstand und Dauer des Auftrags

(1) **Gegenstand**
Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den

1

Objet et durée de la mission

(1) **Objet**
L'objet de la mission, en matière de traitement des données, consiste

Auftragnehmer: Verarbeitung von personenbezogenen Daten im Bereich SAAS Tool (bookingkit Plattform) zur Erfüllung der vom Auftraggeber bezahlten Leistungen im Bereich Vermarktung, Verwaltung und Verkauf seiner Angebote

pour le fournisseur à réaliser les tâches suivantes :
le traitement des données personnelles dans l'outil SAAS Tool (plateforme de bookingkit) en vue de mener à bien les prestations payées par le fournisseur dans les domaines du marketing, de la gestion et de la vente de ses offres

(2) **Dauer**
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der bestehenden Leistungsvereinbarung.

(2) **Durée**
La durée de la présente mission (période) correspond à la période de l'accord de prestations de services existant.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

(3) Les modifications et compléments au présent accord et à tous ses composants - y compris toute assurance du fournisseur - nécessitent un accord écrit ou sous forme électronique contenant une référence explicite au fait que le présent accord a été modifié ou actualisé.

2

Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der vorgesehenen Verarbeitung von Daten**

- Zweck 1 - Geschäftsmodell des Auftraggebers darstellen / Angebot des Dienstes:

  Technische Lösung, um das Geschäftsmodell des Auftraggebers abbilden zu können; dies beinhaltet sowohl die Erstellung von Erlebnissen auf der bookingkit Plattform als auch die technische Abbildung der Konditionen, des gewünschten Buchungsvorganges, des Kommunikationsprozesses mit den Endkunden und zusätzlicher Unternehmensprozesse des Verantwortlichen

2

Concrétisation du contenu de la mission

(1) **Nature et objectifs du traitement prévu des données**

- Objectif 1 : décrire le modèle commercial du client / l'offre de services :

  Solution technique en vue de cartographier le modèle commercial du client ; cela comprend la création d'expériences sur la plateforme de bookingkit ainsi que la représentation technique des conditions, du processus de réservation souhaité, du processus de communication avec le client final et des processus d'entreprise supplémentaires de la personne responsible

- Zweck 2 - Verwaltung des Treuhandkontos:

  Verwaltung des Treuhandkontos des Auftraggebers, um Zahlungen für ihn zu akzeptieren und Auszahlungen zu verarbeiten;

- Zweck 3 - Übermittlung von Informationen zu Diensten des Auftragnehmers:

  Informationen über Änderungen der Dienste des Auftragnehmers übermitteln, die dem Auftraggeber dazu dienen, sein Geschäft effizienter/effektiver abzuwickeln.

- Zweck 4 - Hilfestellung Service-Team:

  Direkte Hilfestellung für die Dienste des Auftragnehmers durch sein Serviceteam auf Anfrage des Auftraggebers oder proaktiv sollte Handlungsbedarf durch den Auftragnehmer festgestellt oder empfohlen sein

- Zweck 5 – Ermöglichung der Vermarktung über Partner

  Technische Lösung, um dem Auftraggeber zu ermöglichen, seine Angebote mithilfe ausgewählter Partnerunternehmen zu vermarkten. Hierzu kann der Auftraggeber die Weitergabe seiner Kontaktdaten und die Daten der von ihm angebotenen Erlebnisse an entsprechende Partner veranlassen, sofern er mit diesen zusammenarbeiten möchte, so dass der Partner mit dem Anbieter für eine Vertragsanbahnung in Kontakt tritt.

- Zweck 6 – Speicherung von Identitätsnachweisen

  Zum Zwecke des vertragsgemäßen Anlegens von Treuhandkonten und zur Ermöglichung der Zusammenarbeit mit Zahlungsanbietern im Rahmen der Vertragserfüllung in Anlehnung an § 11 Geldwäschegesetz sowie zum Zwecke des Nachweises von Prüfungen von hoheitlich erstellten Sanktionslisten.

- Objectif 2 : gestion du compte fiduciaire

  Gestion du compte fiduciaire du client, afin de pouvoir accepter des paiements en son nom et de pouvoir procéder à des remboursements ;

- Objectif 3 : transmission d'informations sur les services du fournisseur :

  Communiquer des informations sur les changements apportés aux services du fournisseur, qui aident le client à développer son entreprise plus efficacement.

- Objectif 4 : assistance de l'équipe Service Client :

  Une assistance directe pour les services du fournisseur par le biais de son équipe Service Client, à la demande du client ou de façon proactive, doit être identifiée ou recommandée par le fournisseur

- Objectif 5 : activation de la commercialisation via des partenaires

  Solution technique permettant au client de commercialiser ses offres avec l'aide de sociétés partenaires sélectionnées.

  À cette fin, le client peut transmettre ses coordonnées et les données des expériences qu'il propose à un partenaire pertinent, s'il souhaite travailler avec lui, afin que ledit partenaire entre en relation avec le fournisseur en vue de préparer un contrat.

- Objectif 6 - Enregistrement des informations d'identification

  Aux fins de mise en place contractuelle de comptes fiduciaires et en vue de permettre la coopération avec les prestataires de services de paiement, dans le cadre de l'exécution du contrat, conformément à l'article 11 de la loi sur le blanchiment d'argent, et aux fins de vérification des listes de sanctions règlementaires.

(2) **Art der Daten -** Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Angaben zur Person:
  - Name
  - Anschrift
  - Geburtsdatum
  - Email Adresse
  - Telefonnnummer
  - Ggf. IBAN
  - Ggf. BIC
  - Ggf. Firmenname
  - Ggf. Steuernummer
  - Ggf. Kopie des Lichtbildausweises
- Online-bezogene Daten:
  - Cookie/ Sitzungsidentifikationsnummer
  - IP Adresse (zur Identifikation bei Vertragsabschluss)
  - Zeitstempel
  - Login-Daten
- Kundendaten:
  - Name
  - E-Mail Adresse
  - Zahlungsart

(3) **Kategorien betroffener Personen** - Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Angestellte
- Auszubildende
- Gewerbliche Mitarbeiter
- Interessenten
- Kunden
- Mitarbeiter
- Praktikanten
- User

(2) **Nature des données :** l'objet du traitement des données personnelles concerne les types/catégories de données suivantes :

- Données personnelles :
  - Nom
  - Adresse postale
  - Date de naissance
  - Adresse e-mail
  - Numéro de téléphone
  - Le cas échéant, IBAN
  - Le cas échéant, BIC
  - Le cas échéant, nom de l'entreprise
  - Le cas échéant, numéro d'identification fiscale
  - Le cas échéant, une copie de la photographie de la pièce d'identité
- Données recueillies en ligne :
  - Cookie / Numéro d'identification de la session
  - Adresse IP (à des fins d'identification à la conclusion du contrat)
  - Horodatage
  - Données de connexion
- Données du client :
  - Nom
  - Adresse e-mail
  - Mode de paiement

(3) **Les catégories des personnes concernées :** les catégories des personnes concernées par le traitement comprennent :

- Les employés
- Les stagiaires
- Les collaborateurs commerciaux
- Les parties intéressées
- Les clients
- Les collaborateurs
- Les apprentis
- Les utilisateurs

3 Technisch-organisatorische Maßnahmen

3 Mesures techniques et organisationnelles

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten

(1) Avant tout traitement, le fournisseur est tenu de documenter la mise en place de mesures techniques et organisationnelles, nécessaires et définies en amont de l'attribution de la mission, en particulier en ce qui concerne l'exécution spécifique de la mission, et remettra ces documents au client pour vérification. Sous réserve de leur acceptation par le client, les mesures documentées deviennent la base du contrat. Dans la mesure où la vérification/l'audit du client nécessite un ajustement, celui-ci doit être mis en œuvre d'un commun accord.

(2) Le fournisseur veille à garantir la sécurité, en vertu de l'article 28, paragraphe 3, alinéa c, et de l'article 32 du RGPD, et en particulier en liaison avec l'article 5, paragraphe 2 du RGPD. De façon globale, les mesures à prendre en compte sont des mesures relatives à la sécurité des données, et la garantie d'un niveau de protection adapté au niveau de risque en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes. Cela implique de prendre en compte l'état de la technique, les coûts de mise en œuvre et la nature, la portée et les objectifs du traitement, ainsi que les diverses probabilités d'occurrence et la gravité du risque envers les droits et les libertés des personnes, au sens de l'article 32, paragraphe 1 du RGPD [Précisions à l'Annexe 1].

(3) Les mesures techniques et organisationnelles sont soumises aux progrès techniques et au développement continu. À cet égard, le fournisseur est habilité à mettre en œuvre des mesures alternatives adéquates. Toutefois, le niveau de sécurité des mesures définies ne pourra être inférieur. Les modifications importantes devront être documentées.

werden. Wesentliche Änderungen sind zu dokumentieren.

4

Berichtigung, Einschränkung und Löschung von Daten

(1) 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. Die Weisung muss schriftlich erfolgen über die Emailadresse datenschutz@bookingkit.de. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

4

Correction, restriction et consentement des données

(1) Le fournisseur ne peut pas décider unilatéralement de corriger, supprimer ou restreindre le traitement des données, réalisé dans le cadre du contrat, mais uniquement conformément aux instructions documentées du client. L'instruction doit être transmise par écrit à l'adresse e-mail suivante : dataprotection@bookingkit.de. Dans la mesure où une personne concernée s'adresse directement au fournisseur à cet égard, ce dernier transmettra immédiatement cette demande au client.

(2) En ce qui concerne l'étendue des prestations, la suppression, le droit à l'oubli, la rectification, la portabilité des données et les informations transmises conformément aux instructions documentées du client, doivent être assurés directement par le fournisseur.

5

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine

5

Assurance qualité et autres obligations du fournisseur

Outre le respect des dispositions de la présente mission, le fournisseur est soumis à des obligations légales conformément à l'article 28 bis 33 du RGPD ; En particulier, il veille tout particulièrement à respecter les exigences suivantes :

a. Demande écrite émanant d'un agent en charge de la protection

Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer die ePrivacy GmbH vertreten durch Prof. Dr. Christoph Bauer, Große Bleichen 21, 20354 Hamburg, telefonisch zu erreichen unter +49 (0) 40 609451810 und per E-Mail über datenschutz@bookingkit.de bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die während des Auftrags und nach dessen Beendigung auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und

des données et qui exerce son droit en vertu des articles 38 et 39 du RGPD.

En tant qu'agent en charge de la protection des données pour le compte du fournisseur, la société ePrivacy GmbH, représentée par le Professeur Christoph Bauer, Große Bleichen 21, 20354 Hambourg, peut être contactée par téléphone au +49 (0) 40 609451810 et par e-mail à l'adresse suivante :dataprotection@bookingkit.de. En cas de changement d'agent en charge de la protection des données, le client doit en être immédiatement informé.

b. Préservation de la confidentialité, conformément aux articles 28, paragraphe 3 S. 2, alinéa b, 29 et 32, paragraphe 4 du RGPD. Le fournisseur s'engage à confier les tâches à réaliser uniquement pendant la durée du contrat et après son échance, à des employés qui sont engagés en matière de confidentialité et qui ont déjà été familiarisés avec les règlements de protection des données pertinents. Le fournisseur et toute personne soumise à son autorité, qui ont accès aux données personnelles, doivent traiter ces données uniquement conformément aux instructions du client, et notamment en vertu des attributions qui leur sont accordées dans le présent contrat, à moins qu'ils ne soient légalement tenus de procéder à leur traitement.
c. Mise en œuvre et respect de toutes les mesures techniques et organisationnelles requises pour ce contrat, conformément à l'article 28, paragraphe 3 S. 2, alinéa c, et à l'article 32 du RGPD [Précisions à l'annexe 1].
d. Le client et le fournisseur collaborent, sur demande, avec l'autorité de surveillance afin de mener à bien leurs missions. tasks.

e. Informer immédiatement le client sur les actions de contrôle et les

Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f. 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.
g. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

mesures prises par l'autorité de surveillance, dans la mesure où elles se rapportent à cette mission. Ceci s'applique également dans le cas où une autorité compétente a établi, dans le cadre d'une procédure administrative ou pénale, le traitement de données à caractère personnel lors du traitement des commandes par le fournisseur.
f. Si toutefois le client est lui-même soumis à un contrôle par l'autorité de surveillance, à une infraction administrative ou pénale, à la responsabilité d'un tiers ou à toute autre réclamation relative au traitement de la commande par le fournisseur, ce dernier est tenu de l'assister au mieux.

g. Le fournisseur contrôle régulièrement les processus internes et les mesures techniques et organisationnelles, afin de veiller à ce que le traitement qui relève de sa responsabilité soit conforme aux exigences de la législation applicable en matière de protection des données et il assure la protection des droits de la personne concernée.

h. Traçabilité des mesures techniques et organisationnelles prises envers le client dans le cadre de ses pouvoirs de contrôle, en vertu de la section 7 du présent contrat.

6

Unterauftragsverhältnisse

(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

6

Contrats de sous-traitance

(1) Au sens de cette règlementation, par contrats de sous-traitance, on entend les prestations de services qui se rapportent directement à la fourniture du service principal. Ceci n'inclut pas les services auxiliaires

der Auftragnehmer 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 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.

fournis par le fournisseur, tels que par exemple les services de télécommunication, les services postaux / de transport, la maintenance et les services aux utilisateurs ou la mise à disposition de supports de données et autres mesures, destinés à assurer la confidentialité, la disponibilité, l'intégrité et les capacités du matériel informatique et des logiciels relatifs aux installations de traitement de données. En revanche, le fournisseur est tenu de s'engager contractuellement et de prendre des mesures de contrôle appropriées et juridiquement conformes, afin d'assurer la protection et la sécurité des données du client, y compris à l'aide de services auxiliaires externalisés.

(2) Die Auslagerung auf Unterauftragnehmer und der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt, wobei die Anzeige auch durch Vorab-Aktualisierung des Anhangs 2 dieser Vereinbarung geschehen kann, welche durch den Auftraggeber in regelmäßigen Abständen geprüft wird, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben, und
- die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) L'externalisation à des sous-traitants et le remplacement du sous-traitant existant sont autorisés, sous réserve que :

(3) Le prestataire soumet ladite externalisation, par écrit et avec un délai de préavis raisonnable, au sous-traitant, étant entendu que la notification peut également être effectuée dans le cadre d´une mise préalable de l'annexe 2 du contrat présent, lequel est examiné par le client à intervalles réguliers, ce qui donne la possibilité à ce dernier de s´opposer à de telles modifications et

(4) les exigences spécifiques des articles 44 et suivants du RGPD oient respectées.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Le transfert des données personnelles du client au sous-traitant et sa première prestation ne sont autorisés que si toutes les conditions préalables à la sous-traitance ont été remplies.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch den Unterauftragnehmern aufzuerlegen.

(6) Si toutefois le sous-traitant fournit le service convenu en dehors de l'UE / EEE, le fournisseur assure la licéité de la protection des données en prenant les mesures appropriées. Il en va de même s'il est fait appel à des prestataires de services, au sens du paragraphe 1, phrase 2.

(7) L'ensemble des dispositions contractuelles dans la chaîne contractuelle doit également être imposé à tout sous-traitant supplémentaire.

7

Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten

7

Droits de contrôle du client

(1) Le client a le droit d'effectuer des vérifications en consultation avec le fournisseur ou de les faire exécuter par des auditeurs à nommer au cas par cas. Il a le droit de s'assurer du respect de cet accord par le fournisseur au sein de son établissement par des vérifications ponctuelles, qui sont généralement notifiées en temps voulu.

(2) Le fournisseur veille à ce que le client soit convaincu du respect des obligations du fournisseur, en vertu de l'article 28 du RGPD. Le fournisseur s'engage à fournir au client les informations nécessaires sur demande et, en particulier, à démontrer la mise en œuvre des mesures techniques et organisationnelles.

(3) La preuve de telles mesures, qui ne concernent pas seulement la mission concrète, peut se faire par

- l'adoption d'un code de conduite approuvé, en vertu de l'article 40 du RGPD ;
- la certification selon une procédure de certification approuvée, en vertu

Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8

Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

de l'article 42 du RGPD ;

- des certificats, rapports ou extraits actuels émanant d'instances indépendantes (par ex. des cabinets d'expertise comptable, d'audit, un service en charge de la sécurité informatique, des auditeurs en charge de la protection des données, des auditeurs qualité) ;

- une certification pertinente par le biais d'un audit de le sécurité informatique ou de la protection des données (par ex. en faisant appel au BSI-Grundschutz).

(4) Le fournisseur peut faire valoir un droit à rémunération afin que les contrôles puissent être effectués par le client.

8

Notification en cas de violation par le fournisseur

(1) Le fournisseur apporte son soutien au client quant au respect de ses obligations relatives à la sécurité des données à caractère personnel, à la notification des violations de données, aux études de l'impact sur la protection de la vie privée et aux consultations préalables, conformément aux articles 32 à 36 du RGPD. Celles-ci incluent, entre autres :

a. la garantie d'un niveau de protection adéquat grâce à des mesures techniques et organisationnelles qui tiennent compte des circonstances et des objectifs du traitement, ainsi que de la probabilité et la gravité prévues d'une violation potentielle des droits en raison de failles dans la sécurité, et de permettre la détection immédiate des incidents de violation

b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen, sofern nicht die Vergütung durch Gesetz dem Auftragnehmer auferlegt wird.

b. l'obligation de signaler immédiatement les violations des données personnelles au client
c. l'obligation de soutenir le client dans la mise à disposition d'informations auprès de la personne concernée et de lui fournir sans délai toutes les informations pertinentes à ce sujet
d. le soutien au client pour son évaluation de l'impact sur la protection de la vie privée
e. le soutien au client dans le cadre de consultations préalables avec l'autorité de surveillance

(2) Pour les services d'assistance qui ne sont pas inclus dans le descriptif des prestations ou qui ne résultent pas d'une faute du fournisseur, ce dernier peut demander à être rémunéré, à moins que la rémunération ne lui soit imposée par la loi.

9

Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9

Pouvoirs du client

(1) Les instructions orales sont immédiatement confirmées par le client (a minima sous forme écrite).

(2) Le fournisseur doit immédiatement informer le client s'il estime qu'une instruction enfreint les règles de protection des données. Le fournisseur est habilité à suspendre l'exécution de l'instruction en question, jusqu'à ce qu'elle soit confirmée ou modifiée par le client.

10

10

Löschung und Rückgabe von personenbezogenen Daten

(1) 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ausgenommen sind Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, welche der Auftragnehmer aufgrund rechtlicher Bestimmungen aufzubewahren hat.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner

Suppression et restitution des données à caractère personnel

(1) Des copies ou des duplicatas des données ne sont pas autorisés sans que le client n'en soit informé. Cela n'inclut pas les copies de sauvegarde, si toutefois elles sont nécessaires pour assurer un traitement adéquat des données, et les données nécessaires au respect des exigences de conservation légales.

(2) Une fois les tâches prévues au contrat réalisées, ou plus tôt sur demande du client et au plus tard à la date résiliation du contrat de prestations de services, le fournisseur doit remettre au client tous les documents, les résultats issus du traitement et de l'utilisation ainsi que toutes les données enregistrées, en rapport avec la mission et en sa possession, ou les détruire conformément à la loi sur la protection des données et après avoir au préalable obtenu l'autorisation du client. La même obligation s'applique aux documents utilisés pour les tests et à tout document résiduel. Le protocole de suppression doit être remis sur demande. Sont exclus les documents, les résultats de traitement et d'utilisation ainsi que les ensembles de données liés à la relation contractuelle que l'entrepreneur doit conserver en raison de la réglementation en vigueur.

(3) Les documents, qui apportent la preuve d'un traitement des données approprié et conforme à la mission, doivent être conservés par le fournisseur conformément aux périodes de conservation respectives et à l'issue de la période du contrat. Il

Entlastung bei Vertragsende dem Auftraggeber übergeben.

peut par ailleurs les remettre au client.

ANLAGE 1
Technisch-organisatorische Maßnahmen

1

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

a. Zutrittskontrolle

- Der Auftragnehmer stellt anhand von elektronischen Schlüsseln sicher, dass nur autorisierte Personen Zutritt zu ihren Räumlichkeiten haben. Diese können individuell gesperrt werden.
- Außerdem ist das Bürogelände des Auftragnehmers 24 Stunden täglich von einem Wachdienst geschützt, welcher regelmäßig Rundgänge durchführt.
- Es ist ein Alarmsystem installiert, welches mit einem Schließmechanismus für die Türen gekoppelt ist.
- Die Tür des Serverraums ist mit einem Schlüssel gesichert, welcher nur dem zuständigen Personal zur Verfügung steht.
- Mitarbeitern im Homeoffice ist es untersagt, außerhalb des Bürogeländes betriebliche Unterlagen auf Papier oder portablen Datenträgern zu nutzen. Daten sind ausschließlich über die zentrale Datenverwaltung zu nutzen.

b. Zugangskontrolle

- Der Auftragnehmer gewährt Mitarbeitern nur auf die Systeme Zugriff, welche er für die

ANNEXE 1
Mesures techniques et organisationnelles

1

Confidentialité (Article 32, paragraphe 1, alinéa b du RGPD)

a. Contrôles des accès physiques

- Le fournisseur utilise des clés électroniques pour s'assurer que seules les personnes autorisées ont accès à ses locaux. Ceux-ci peuvent être verrouillés individuellement.
- Par ailleurs, les bureaux du fournisseur sont protégés 24 heures sur 24 par un service de sécurité qui effectue des visites régulières.
- Un système d'alarme est installé, qui est couplé avec un mécanisme de fermeture des portes.
- La porte de la salle des serveurs est sécurisée à l'aide d'une clé qui n'est accessible qu'aux personnes appropriées.
- Les employés du bureau à domicile ne sont pas autorisés à utiliser les documents de l'entreprise sur du papier ou des dispositifs de stockage de données portables à l'extérieur des bureaux. Les données ne peuvent être utilisées que via le système central de gestion des données.

b. Contrôles des accès au système

- Le fournisseur accorde à chaque collaborateur uniquement un accès aux systèmes qui lui sont

Ausführung seiner konkreten Aufgaben benötigt.

- Den Zugang zu den eigenen Systemen regelt der Auftragnehmer über sichere personalisierte Passwörter und Passwortverfahren. Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account geknüpft. Außerdem verfügen alle Mitarbeiter des Auftragnehmers über ein Passwortmanagementsystem, welches im Bedarfsfall zufällige Passwörter für sensible Systeme festlegt.
- Passwörter des Auftragnehmers unterliegen Mindestanforderungen an Sicherheitsbestimmungen.
- Alle Datenträger und Laptops sind verschlüsselt.
- Alle Windows Laptops nutzen die Full Disk Hardware Encryption der verbauten SSDs. Alle Macbooks nutzen die integrierte Filevault Encryption von MacOS.
- Alle Computer verfügen über Virenscanner, welche täglich geupdated werden.

c. Zugriffskontrolle

- Zugangsberechtigte können nur auf Daten zugreifen, die in ihrem individuellen Berechtigungsprofil eingerichtet sind.
- Zum Erstellen und Ändern von Berechtigungsprofilen gibt es strenge Regelungen und Verfahren, welche die Genehmigung durch die Geschäftsführung einschließen.
- Das Sperren bzw. Abmelden beim Verlassen des Arbeitsplatzes ist

nécessaires pour mener à bien ses tâches spécifiques.

- Le fournisseur réglemente l'accès à ses propres systèmes via des mots de passe personnalisés sécurisés et des procédures de mot de passe. Les autorisations sont liées à un identifiant utilisateur personnel et à un compte. Par ailleurs, tous les collaborateurs du fournisseur disposent d'un système de gestion des mots de passe, qui, le cas échéant, détermine des mots de passe aléatoires pour les systèmes sensibles.
- Les mots de passe du fournisseur sont soumis à des exigences de sécurité minimales.
- Tous les supports de données et les ordinateurs portables sont verrouillés.
- Tous les ordinateurs portables sous Windows utilisent le chiffrement complet du disque dur (Full Disk Hardware Encryption) des SSD intégrés. Tous les Macbooks utilisent le chiffrement intégré Filevault de MacOS.
- Tous les ordinateurs disposent de scanners de virus, mis à jour quotidiennement.

c. Contrôles d'accès aux données

- Les bénéficiaires peuvent uniquement accéder aux données qui sont définies dans leur profil d'autorisation individuel.
- Pour créer et modifier les profils d'autorisation, il existe des règles et des procédures strictes qui incluent l'approbation de la direction.
- Le verrouillage ou la déconnexion lorsque l'on quitte

schriftlich angeordnet und wird praktiziert.

- Alle Server und Services des Auftragnehmers werden kontinuierlich überwacht.

d. Trennungskontrolle

- Berechtigungskonzepte verhindern die ungeplante Verwendung sensibler Daten. Der Zugriff auf die Daten selbst ist zudem dadurch eingeschränkt, dass die Mitarbeiter Services (Applikationen) verwenden, welche den Zugriff steuern und kein Beschreiben der Daten zulassen.

- Alle Kundendaten werden in der selben Datenbank verwaltet, da es systembedingt nicht möglich ist diese auf Datenbankebene zu trennen. Da ohnehin ausschließlich über entsprechende Software auf die Daten zugegriffen werden darf, wird Trennung über ein Rollenkonzept in der Software sichergestellt.
  Ausnahmen gelten für Developer und das Customer Success Team, die zur Fehlerbehebung direkt auf die Datenbank zugreifen dürfen. Dieser Zugriff erfolgt ausschließlich lesend, so dass keine Daten am Rollenkonzept vorbei verändert werden können.

- Es gibt ein abgetrenntes WLAN für Gäste.
- Es erfolgt eine Trennung von Test- und Produktivsystemen. Sollten Softwareneuerungen der Trennungskontrolle nicht genügen, werden diese im Testsystem aufgedeckt und nicht in das Produktivsystem übernommen.

son poste de travail fait l'objet d'une procédure écrite et est pratiqué.

- Tous les serveurs et les services du fournisseur sont surveillés en permanence.

d. Contrôles des séparations

- Les concepts d'autorisation empêchent l'utilisation non prévue de données sensibles. L'accès aux données est également limité par le fait que les collaborateurs utilisent des services (applications) qui contrôlent l'accès et ne permettent pas l'écriture des données.

- Toutes les données client sont gérées dans la même base de données ; il n'est pas possible de les séparer au niveau de la base de données en raison du système. Les données ne pouvant être consultées qu'avec un logiciel approprié, la séparation est assurée par un concept de rôles dans le logiciel. Des exceptions s'appliquent aux développeurs et à l'équipe Service Client, qui sont autorisés à accéder directement à la base de données à des fins de résolution des problèmes. Cet accès est en lecture seule, de sorte qu'aucune donnée ne puisse être modifiée lors du concept de rôles.

- Nous disposons d'une connexion wifi séparée pour les visiteurs.
- Il existe par ailleurs une séparation des systèmes de tests et de production. Si les mises à jour logicielles du contrôle de séparation ne suffisaient pas, elles seront découvertes au niveau du système de test et ne seront pas transférées dans le système de production.

e. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Daten für interne Auswertungen zu statistischen Zwecken zur Produktivitätssteigerung werden vor der Verarbeitung anonymisiert indem die IP Adressen gekürzt bzw. zufällig verändert werden.

- Insbesondere im Bereich des Onlinemarketings wird ausschließlich mit pseudonymen Online-Identifiern und -Profilen gearbeitet. Diese werden mittels des sogenannten hashings pseudonymisiert

e. Pseudonymisation (Article 32, paragraphe 1, alinéa a du RGPD ; Article 25, paragraphe 1 du RGPD)

- Les données nécessaires aux évaluations internes à des fins statistiques, afin d'augmenter la productivité, sont pseudonymisées avant le traitement, en raccourcissant les adresses IP ou en les modifiant de façon aléatoire.

- En particulier dans le domaine du marketing en ligne, nous utilisons exclusivement des identifiants et des profils en ligne pseudonymisés. Ceux-ci sont pseudonymisés à l'aide du hachage.

2

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

a. Weitergabekontrolle

- Alle Transportwege sind SSL-verschlüsselt.
- Das Rechtemanagement für die Datenauslesung des Auftraggebers liegen beim Auftraggeber.
- Der Verkehr zwischen den Systemen ist über SSL/TLS verschlüsselt.
- Das Frontend verfügt über eine Https-Verschlüsselung.
- Der Zugang zu den Systemen von außen ist über open VPN verschlüsselt. Mitarbeiter mit VPN Zugang müssen sich über Benutzername/Passwort und ein Zertifikat authentifizieren.

- Hardwarekomponenten oder Dokumente werden so vernichtet, dass eine Wiederherstellung nicht oder nur mit unverhältnismäßigem

2

Confidentialité (Article 32, paragraphe 1, alinéa b du RGPD)

a. Contrôles des transferts

- Tous les supports de transfert sont dotés d'un cryptage SSL.
- La gestion des droits pour la lecture des données du client revient au client.
- Le transfert entre les systèmes est doté d'un cryptage SSL/TLS.

- Le Front-End dispose d'un cryptage Https.
- L'accès au système depuis l'extérieur est chiffré par le biais d'un VPN ouvert. Les collaborateurs disposant d'un accès VPN doivent s'identifier à l'aide d'un nom d'utilisateur/mot de passe et d'un certificat.

- Les composants informatiques ou les documents sont détruits de façon à rendre impossible une quelconque restauration, ou

Aufwand möglich ist.

- Die Datenübertragung zwischen Clients und Servern erfolgt verschlüsselt.
- Für die Anfertigung von Kopien gibt es eindeutige Regelungen und Verfahrensweisen.
- Es existieren mehrere Firewalls.
- Auf sämtlichen Arbeitsstationen existieren Firewalls, welche ständig aktiviert sind und durch den Nutzer nicht deaktivierbar sind.

b. Eingabekontrolle

- Die Mitarbeiter außerhalb der Entwicklungsabteilung des Auftragnehmers arbeiten nicht direkt auf Datenbankebene, sondern nutzen Applikationen, um auf die Daten zuzugreifen.
- Datenbankstrukturänderungen werden detailliert im Projektmanagementtool JIRA protokolliert. Die Protokolle werden revisionssicher 12 Monate lang aufbewahrt. Die Eingabe, Änderung und Löschung von Daten kann dabei anhand von individuellen Benutzernamen nachvollzogen werden.
- IT-Mitarbeiter verwenden einen gemeinsamen Login für die Datenbanken, da es wenige Mitarbeiter sind, die räumlich beieinander sitzen. Durch Absprachen und Sichtkontrollen wird die Arbeit an den Datenbanken zusätzlich überwacht.

uniquement avec des efforts disproportionnés.

- Le transfert de données entre les clients et les serveurs s'opèrent de façon cryptée.
- Il existe des règles et des procédures claires pour la réalisation de copies.
- De nombreux pare-feux sont installés.
- Des pare-feux sur tous les postes de travail sont activés en permanence et ne peuvent pas être désactivés par l'utilisateur.

b. Contrôles de saisie

- Les collaborateurs extérieurs au département de développement du fournisseur ne travaillent pas directement au niveau de la base de données, mais utilisent des applications pour accéder aux données.
- Les modifications apportées à la structure de la base de données sont détaillées dans l'outil de gestion de projet JIRA. Les journaux peuvent être vérifiés pendant 12 mois. La saisie, la modification et la suppression des données peuvent être tracées à l'aide de noms d'utilisateur individuels.
- Le personnel informatique utilise un identifiant commun pour les bases de données, dans la mesure où ils sont peu nombreux et où ils sont les uns à côté des autres. Les tâches effectuées sur les bases de données sont également surveillées par le biais de dispositifs et de contrôles visuels.

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

Verfügbarkeitskontrolle

- Der Auftragnehmer erstellt täglich ein weiteres Gesamt-Backup, welches für 7 Tage gespeichert wird. Auf diese Backups kann zurückgegriffen werden, sollten andere Verfügbarkeitsmaßnahmen versagen. Es handelt sich hierbei um ein Gesamtbackup, welches nicht zur Wiederherstellung einzelner Daten herangezogen werden kann, sondern lediglich das komplette System wiederherstellt.
- Aus diesen Backups kann jederzeit im Falle eines Notfalls das System wiederhergestellt werden.
- Es existiert ein Notfallplan, aus welchem hervor geht, welche Schritte wann eingeleitet werden müssen und welche Personen und Stellen zu welchem Zeitpunkt und welchem Zweck informiert werden müssen.
- Die einzelnen Arbeitsstationen beim Auftragnehmer sind über täglich geupdatete Virenscans geschützt, die Datenträger sind verschlüsselt.
- Unsere Server und Backup-Systeme stehen in den Rechenzentren von Amazon Web Services welche umfassend für die Betriebskontinuität geschützt sind. Details dazu können sie hier nachlesen: https://aws.amazon.com/de/compliance/data-center/controls/
- Hochverfügbare Systeme werden parallel in mehreren Rechenzentren redundant betrieben.
- Die Überlastung von Servern ist durch eine sogenannte autoscaling group ausgeschlossen. Steigt die Last auf die Server werden automatisiert weitere

Confidentialité et résilience (Article 32, paragraphe 1, alinéa b du RGPD)

Contrôles de disponibilité

- Le fournisseur crée une sauvegarde supplémentaire quotidienne, qui est stockée pendant 7 jours. Ces sauvegardes peuvent être utilisées si d'autres mesures de disponibilité échouent. Il s'agit d'une sauvegarde complète, qui ne peut pas être utilisée pour restaurer des données individuelles, mais uniquement pour restaurer l'ensemble du système.
- A partir de ces sauvegardes, le système peut être restauré à tout moment en cas d'urgence.
- Il existe un plan d'urgence qui décrit les étapes à suivre, ainsi que les personnes et les fonctions qui doivent être informées, à quel moment et dans quel but.
- Les postes de travail individuels du fournisseur sont protégés par des analyses antivirus quotidiennes, et les supports de données sont cryptés.
- Nos serveurs et systèmes de sauvegarde sont situés dans les centres de données Amazon Web Services, et sont ainsi entièrement protégés pour la continuité de l'activité. Pour toute information complémentaire, vous pouvez consulter le site suivant : https://aws.amazon.com/fr/compliance/data-center/controls/
- Les systèmes à disponibilité élevée sont exploités de manière redondante, en parallèle, dans plusieurs centres de données.
- La surcharge des serveurs est exclue grâce au groupe Auto Scaling. Si la charge sur les serveurs augmente, des serveurs supplémentaires sont

Server hinzu geschaltet, um eine Überlastung zu verhindern.

- Sämtliche Betriebsparameter werden permanent überwacht.

automatiquement ajoutés pour éviter toute surcharge.

- Tous les paramètres de fonctionnement sont surveillés en permanence.

4

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

a. Datenschutz Management

- Der Auftragnehmer überprüft regelmäßig ihr Datenschutz-Management unter Einbeziehung des betrieblich bestellten Datenschutzbeauftragten.
- Sämtliche Mitarbeiter werden regelmäßig zum Thema Datenschutz geschult. Außerdem werden alle Mitarbeiter auf das Datengeheimnis verpflichtet. Mitarbeiter im Homeoffice werden auf die besonderen Regeln gesondert belehrt

b. Incident Response Management

- Im Falle einer Datenpanne greift ein umfassendes Regelwerk zu einzuleitenden Prozessen und Kommunikationsschritten.
- Für die gegebenenfalls zu erfolgende Information von Aufsichtsbehörden sind die verantwortlichen Mitarbeiter geschult, so dass einer Information innerhalb von 72 Stunden nichts im Wege steht.

c. Datenschutzfreundliche Voreinstellungen

- Bei der Entwicklung jeder Technologie oder jedes neuen Produktes wird von vornherein ein Privacy by Design-Ansatz verfolgt. Es wird von vornherein das Ziel

4

Procédures d'examen périodique, d'évaluation et d'analyse (Article 32, paragraphe 1, alinéa d du RGPD ; Article 25, paragraphe 1 du RGPD)

a. Gestion de la protection des données

- Le fournisseur vérifie régulièrement sa gestion de la protection des données, sous le contrôle du responsable de la protection des données désigné.
- L'ensemble du personnel est régulièrement formé à la protection des données. Par ailleurs, tous les collaborateurs s'engagent à respecter la confidentialité des données. Les employés travaillant depuis leur domicile recoivent des instructions séparées sur les règles spéciales.

b. Gestion de la réponse aux incidents

- En cas de violation de données, un ensemble complet de règles s'applique aux processus et aux étapes de communication à mettre en œuvre.
- Les employés responsables sont formés pour que les informations puissent être fournies par les autorités de surveillance, de sorte que l'information puisse être transmise dans les 72 heures.

c. Réglages par défaut conformes à la protection de la vie privée

- Lors du développement d'une technologie ou d'un nouveau produit, une approche fondée sur la confidentialité est suivie dès le départ. Dès le départ,

verfolgt, die Menge der zu erhebenden Daten zu minimieren und den Umfang der Datenverarbeitung zu reduzieren

- Soweit möglich werden Daten nur pseudonymisiert weiterverarbeitet. Datenschutzerklärungen, welche leicht zugänglich sind und sämtliche Datenprozesse ausführlich beschreiben, sorgen für Transparenz.

d. Auftragskontrolle

- Sämtliche Auftragnehmer sind unter Sorgfaltsgesichtspunkten ausgewählt.
- Mit sämtlichen Auftragnehmers werden Auftragsverarbeitungsverträge abgeschlossen und technische und organisatorische Maßnahmen werden regelmäßig überprüft.
- Kontrollrechte werden mit Auftragnehmern vertraglich vereinbart.

l'objectif est de minimiser la quantité de données à collecter et de réduire la quantité de données traitées.

- Dans la mesure du possible, les données sont traitées uniquement sous forme pseudonymisée. Les déclarations de confidentialité, qui sont facilement accessibles et détaillent tous les processus de données, veillent à la transparence nécessaire.

d. Contrôles de la mission

- L'ensemble des fournisseurs est sélectionné avec soin.
- Des contrats de traitement des données sont signés avec tous les fournisseurs et les mesures techniques et organisationnelles sont régulièrement revues.
- Les droits de contrôle sont convenus avec les fournisseurs dans le cadre d'un contrat.

ANLAGE 2
Unterauftrags-verhältnisse

Präambel

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 Auftragnehmer 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.

1

Bestehende Unterauftragsverhältnisse

Eine Liste von bestehenden Unterauftragsverhältnisse ist unter folgendem Link abrufbar: https://bookingkit.net/legaldocuments-dpa-list

ANNEXE 2
Contrats de sous-traitance

Préambule

Au sens de cette règlementation, par contrats de sous-traitance, on entend les prestations de services qui se rapportent directement à la fourniture du service principal. Ceci n'inclut pas les services auxiliaires fournis par le fournisseur, tels que par exemple les services de télécommunication, les services postaux / de transport, la maintenance et les services aux utilisateurs ou la mise à disposition de supports de données et autres mesures, destinés à assurer la confidentialité, la disponibilité, l'intégrité et les capacités du matériel informatique et des logiciels relatifs aux installations de traitement de données.

1

Contrats de sous-traitance existants

La liste des contrats de sous-traitance peut être trouvée avec le lien suivant : https://bookingkit.net/legaldocuments-dpa-list

2

Bestehende Unterauftrags-verhältnisse mit Unternehmen aus Drittländern

Eine Liste von bestehenden Unterauftragsverhältnisse mit Unternehmen aus Drittländern ist unter folgendem Link abrufbar: https://bookingkit.net/legaldocuments-dpa-list-2/

2

Contrats de sous-traitance existants avec des entreprises basées dans des pays tiers

La liste des contrats de sous-traitance avec des entreprises basées dans des pays tiers peut être trouvée avec le lien suivant : https://bookingkit.net/legaldocuments-dpa-list-2/