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

ContractHero GmbH
vertreten durch / *represented by*
Sebastian Wengryn und Gerry C. Koch Kiautschoustraße 14
D-13353 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:

"ContractHero App":
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:

"ContractHero 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

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 (ContractHero App) zur Erfüllung der vom Auftraggeber bezahlten Leistungen im Bereich Verwaltung von Verträgen

(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 die Erstellung von Erinnerungen und Eintragung von vertragsrelevanten Details auf der ContractHero App als auch die technische Abbildung der Dokumente und Informationen, Übertragung der gewünschten Erinnerungen, des Kommunikationsprozesses mit den Kunden und zusätzlicher Unternehmensprozesse des Verantwortlichen

be performed by the Supplier: processing personal data in the area of SaaS Tool (the ContractHero platform) to fulfil the services paid for by the Client in the area of management of contract.

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

(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

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; his includes the creation of reminders and entry of contract-relevant details on the ContractHero app as well as the technical mapping of documents and information, transmission of the desired reminders, the communication process with customers and additional business processes of the responsible party.

- Zweck 2 - Übermittlung von Informationen zu Diensten des Auftragnehmers:

  Informationen über Änderungen der Verträge des Auftragnehmers übermitteln, die dem Auftraggeber dazu dienen, seine Verträge und Dokumente besser zu managen

- Zweck 3 - 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.

- Purpose 2 - communication of information regarding the services provided by the Supplier

  Communicating information about changes to the Contracts provided by the Supplier, which the Client can use to run its business better

- Purpose 3 - 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.

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

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

(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.
  - Company name
  - Tax number (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

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,

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

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@contracthero.de. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

(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

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:

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. 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. 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].

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

d. 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

a. 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.

b. 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].

c. The Client and the Supplier will work together with the supervisory authority on request to fulfil their tasks.

d. 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.

e. 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.

f. 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.

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

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

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.

e. 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.

f. 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.

g. 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

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:

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

- 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

- 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

- die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

- 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.

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);

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

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.

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

- 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

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.

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

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

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

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

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.

- 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.

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

- 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

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.