



Auftragsverarbeitungsvertrag

gemäß Artikel 28 Abs. 9 DSGVO

Hinweis zur Vertragssprache:

Dieser Auftragsverarbeitungsvertrag ist in Deutsch und Englisch geschrieben. Im Fall von Widersprüchen geht die deutsche Version vor.

Hinweis zum nDSG (Schweiz):

Ab dem 01.09.2023 gilt in der Schweiz das neue Datenschutzgesetz (nDSG), das in vielen Teilen mit der europäischen DSGVO übereinstimmt. Der Hauptunterschied zur DSGVO ergibt sich vor allem in der persönlichen Haftung des Auftraggebers bei Datenschutzverletzungen.

Sofern das beauftragende Unternehmen (Auftraggeber) in der Schweiz ansässig ist und zusätzlich zu diesem Auftragsverarbeitungsvertrag deshalb ergänzende Absprachen wünscht, können diese in Übereinstimmung mit dem Auftragnehmer im Rahmen einer Nebenabrede vereinbart und diesem Auftragsverarbeitungsvertrag hinzugefügt werden. Wenden Sie sich hierzu bitte an datenschutz@cisbox.com.

Data processing agreement

according to article 28 para. 9 GDPR

Note on language:

This data processing agreement is written in German and in English. In the event of a discrepancy, the German version shall prevail.

Information about nFADP (Switzerland):

As of 01.09.2023, the new Federal Act on Data Protection (nFADP) will apply in Switzerland, which is equivalent in many parts to the European GDPR. Primarily, the main difference to the DSGVO arises in the personal liability of the customer, which may result from data protection violations.

If the commissioning company (customer) is located in Switzerland and requires additional arrangements beyond this DPA, these arrangements can be concluded in cooperation with the contractor as part of a side agreement and added to this DPA. For this purpose, please contact dataprotection@cisbox.com.

nachfolgend „Auftraggeber“

Firmendaten in Übereinstimmung mit den Geschäftsdaten des diesem AV-Vertrag zugrunde liegenden Nutzungsbedingungen. Sofern der Auftraggeber auf Grundlage des Nutzungsbedingungen auch anderen (z. B. verbundenen) Unternehmen die Nutzung der vereinbarten Applikationen, Dienstleitungen und / oder Services einräumt, so hat der Auftraggeber seinerseits eine Vereinbarung zur Auftragsverarbeitung im Innenverhältnis mit diesen Unternehmen getroffen.

hereinafter “customer”

Company data in accordance with the commercial information of the service contract underlying this data processing agreement. If the customer also grants other (e.g. connected / affiliated) companies the usage of the agreed applications and / or services on basis of the service contract, the customer has in turn entered into an agreement on data processing with these companies.

zwischen | between

Firmenname / Company name

Straße und Hausnummer / Street and Number

Postleitzahl / Postcode

Stadt / City

und | and

cisbox GmbH

Brühler Straße 58

D-42657 Solingen

Germany

Telefon | Phone: +49 (0)212 / 2315 - 0

E-Mail: datenschutz@cisbox.com | Email: dataprotection@cisbox.com

Web: <https://www.cisbox.com>

Amtsgericht | District court: Wuppertal HRB 19187

UST-ID | VAT-ID: DE243208591

Geschäftsführer | Managing directors: Christof Majer

nachfolgend „Auftragnehmer“

hereinafter “contractor”

Präambel

Die Vertragspartner schließen diesen Auftragsverarbeitungsvertrag (nachfolgend „AVV“) in Ansehung der ab dem 25.05.2018 geltenden EU-Datenschutzgrundverordnung (DSGVO).

1 Anleitung

(1) Dieser AVV wurde durch den Auftragnehmer erstellt und wirkt für den Auftragnehmer gem. DSGVO Art. 28 Abs. 9 seitens des Auftraggebers als (vor)unterzeichnet. Die folgenden Voraussetzungen sind erforderlich, damit dieser AVV gültig wird:

- a) Es muss ein Vertragsverhältnis im Sinne des zugrunde liegenden Nutzungsbedingungen bestehen
- b) Der AVV muss im dafür vorgesehenen Unterschriftenfeld unterzeichnet sowie alle mit *Stern gekennzeichneten Stellen vervollständigt werden
- c) Der vervollständigte muss AVV postalisch, als Scan per E-Mail oder über eine geeignete Signatlösung (z. B. FP Sign) an den Auftragnehmer übermittelt werden

2 Wirksamkeit

- (1) Dieser AVV wird (zum Datum des Inkrafttretens) nur dann wirksam, wenn er vollständig und in Übereinstimmung mit Art. 1 und Art. 2 dieses AVVs an den Auftraggeber übermittelt wird.
- (2) Der Unterzeichner des Auftraggebers erklärt gegenüber dem Auftragnehmer, dass er oder sie die rechtliche Befugnis hat, Verträge in Vertretung des Auftraggebers abzuschließen.

3 Gegenstand und Dauer des AVVs

- (1) Der Gegenstand ergibt sich aus dem diesem AVV zugrunde liegenden Nutzungsbedingungen.
- (2) Die Dauer (Laufzeit) dieses AVV entspricht der Laufzeit des zugrunde liegenden Nutzungsbedingungen, sofern sich aus den Bestimmungen dieser Vereinbarung sowie aus gesetzlichen Aufbewahrungsfristen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.
- (3) Dieser AVV tritt mit Vertragsunterschrift durch beide Parteien in Kraft.

4 Umfang, Art und Zweck der Datenverarbeitung, die Datenarten und der Kreis der Betroffenen

- (1) Die Tätigkeit des Auftragnehmers ergibt sich aus dem diesem AVV zugrunde liegenden Nutzungsbedingungen.

Preamble

The contracting partners enter into this data processing agreement (hereinafter "DPA") in light of the EU Data Protection Regulation (GDPR) in force as of 25.05.2018.

1 Instructions

(1) This contract has been prepared by the Contractor and is deemed to have been pre-signed by the Contractor according to article 28 para. 9 GDPR. The following requirements are necessary for this DPA to become valid:

- a) there must be a contractual relationship within the meaning of the underlying service contract
- b) the DPA must be signed in its purposed signature field and all spaces marked with *asterisk must be completed
- c) the completed DPA must be sent to the contractor by mail or transmitted as a scan by email or via a qualified signature solution (e.g. FP Sign)

2 Effectiveness

- (1) This DPA shall become effective (as of the effective date) only if it is transmitted to contractor in its entirety and in accordance with article 1 and 2 of this DPA.
- (2) The customer's signatory declares to the contractor that he or she has the legal authority to conclude contracts on behalf of the customer.

3 Object and duration of the DPA

- (1) The object results from the service contract underlying this DPA.
- (2) The duration (term) of this DPA corresponds to the term of the underlying service contract, unless the provisions of this Agreement and statutory retention periods impose obligations or termination rights beyond that term.
- (3) This DPA shall enter into force upon signature by both parties to the service contract.

4 Scope, nature and purpose of data processing, types of data and affected parties

- (1) The activities of the contractor result from the service contract underlying this DPA.

(2) Die Verarbeitung und Nutzung der Daten kann **je nach Kunde und Auftrag** im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, sowie im Drittland Vietnam stattfinden. Das angemessene Schutzniveau im Drittland Vietnam wird sowohl durch die neuen Standardvertragsklauseln mit Gültigkeit ab dem 27.12.2022 (Artikel 46 Absatz 2 lit. c und d DSGVO) als auch durch weitere technische und organisatorische Maßnahmen hergestellt, die insgesamt ein angemessenes Datenschutzniveau gewährleisten. Zudem versichert der Auftragnehmer die Einhaltung des Europäischen Datenschutzrechts. Der Auftraggeber stimmt dieser Verarbeitung und Nutzung der Daten in diesem Drittland Vietnam zu.

(3) Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff DSGVO erfüllt sind.

(4) Gegenstand der Erhebung und regelmäßigen Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten:

- Personenstammdaten
(Vor- und Nachname, Geschlecht, Titel, Funktion, Berufsbezeichnung)
- Kommunikationsdaten
(Adresse, Telefon, E-Mail, Fax, Mobiltelefon)
- Vertragsstammdaten
(Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten

(5) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses AVVs Betroffenen umfasst:

- Lieferanten
- Kunden
- Kontaktpersonen
- Mitarbeiter als Nutzer der Applikationen

5 Weisungsbefugnis des Auftraggebers und Remonstration

(1) Weisungen des Auftraggebers werden ausschließlich in schriftlicher Form an die Geschäftsführung oder den/die jeweilige(n) Ansprechpartner(in) des Auftragnehmers gerichtet.

(2) Weisungen, die nicht in diesem AVV vorgesehen oder durch die DSGVO geregelt sind, werden als Antrag auf Leistungsänderung behandelt.

(2) The processing and use of data can, **depending on customer and order**, take place within the territory of the Federal Republic of Germany, a member state of the European Union, in another treaty country of the agreement on the European Economic Area, or the third country Vietnam. The appropriate protection level in the third country is established both by the new Standard Contractual Clauses valid from 27.12.2022 (article 46 para. 2 lit. c and d GDPR). and by technical and organizational measures that ensure an adequate level of data protection. In addition, the contractor assures compliance with European data privacy law. The customer agrees to this processing and use of data in this third country Vietnam.

(3) Any transfer to another third country requires the prior approval of the customer and may only take place if the conditions of articles 44 ff (and following) GDPR are met.

(4) The following types of data are the object of collection and regular processing and / or use of personal data:

- Person master data
(first name, surname, gender, title, function, job title)
- Communications data
(address, telephone, email, fax, mobile phone)
- Contract master data
(contractual relationship, product and contractual interests)
- Contract account- and payment data
- Planning- and tax data

(5) The groups of persons affected by handling their personal data in the context of this DPA include:

- Suppliers
- Customers
- Contact persons
- Employees as users of the applications

5 Authority of the customer and remonstration

(1) Customer instructions are addressed in written form only to the contractor's management or the respective contact persons.

(2) Instructions that are not included in this DPA or regulated by the GDPR shall be treated as a request for agreement modification.

- (3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach seiner Ansicht gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt (Remonstration). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Dies begründet keine Prüfpflicht des Auftragnehmers bzgl. erhaltener Weisungen des Auftraggebers.

6 Vertraulichkeits- / Verschwiegenheitspflicht

- (1) Der Auftragnehmer wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

- (1) Der Auftragnehmer ergreift alle geeigneten technischen und organisatorischen Maßnahmen gem. Artikel 32 DSGVO.
- (2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses AVVs sind diese durch den Auftragnehmer fortlaufend an die Anforderungen dieses AVVs anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der in dieser AVV festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.
- (3) Die Einzelheiten der technischen und organisatorischen Maßnahmen haben die Vertragspartner in **Anlage 2** zu diesem AVV vereinbart.

8 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 folgende Nebenleistungen, die der Auftragnehmer etwaig in Anspruch nimmt:
- a) Telekommunikationsdienstleistungen, Post- / Transportdienstleistungen, Wartung und Benutzerservice, Entsorgung von Datenträgern
 - b) Serviceleistungen zur Ermöglichung von Funktionen wie z. B. Verifikation, Authentifizierung, ext. Datenabruf, Support (Helpdesk) oder ähnlich
 - c) sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen

- (3) The contractor will immediately inform the customer if he deems the implementation of an instruction from the customer would in his opinion result in a violation of GDPR or of another data protection regulation (remonstration). The contractor is entitled to suspend implementation of such an order until it is confirmed or modified by the customer. This does not result in an inspection obligation for the contractor with regard to received customer instructions.

6 Confidentiality- and secrecy obligations

- (1) The contractor shall only employ persons for contract execution who have been obligated to maintain confidentiality or who are subject to a statutory obligation of secrecy.

7 Security of processing / technical and organisational measures according to article 32 GDPR

- (1) The contractor takes all appropriate technical and organisational measures according to article 32 GDPR.
- (2) Technical and organisational measures are subject to technical advances and continued development. For the duration of this DPA, these shall continuously be adapted to requirements of this DPA by the contractor and developed according to technical progress. The security level of the technical and organisational measures defined in this DPA must not decrease.
- (3) The contracting partners have agreed the details of technical and organisational measures in **Annex 2** of this OP agreement.

8 Sub-contractual relations

- (1) Services that relate directly to the performance of the main service are considered sub-contractual in terms of this provision. They do not include the following ancillary services the contractor uses:
- a) telecommunication services, postal- and transport services, maintenance and user services, disposal of data carriers
 - b) services for enabling functions such as verification, authentication, ext. data retrieval, support (helpdesk) or similar
 - c) other measures that ensure confidentiality, availability, integrity and capacity of the hard- and software of data processing systems.

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

- (2) Der Auftragnehmer wird die mit diesem AVV übernommenen Verpflichtungen dem Subunternehmen selbständig auferlegen. Der Unterauftrag ist schriftlich zu fixieren. Der Auftragnehmer bleibt gegenüber dem Auftraggeber verantwortlich. Bei den meisten zur Vertragsdurchführung eingesetzten Unterauftragnehmern handelt es sich um innerhalb der Unternehmensgruppe verbundene Unternehmen mit einer Kapitalbeteiligung von über 50 % oder beherrschendem Einfluss („Unternehmensgruppe“ gemäß Art. 4 Abs. 19 DSGVO). Zwischen den Unternehmen der Unternehmensgruppe sind zudem ihrerseits AVV geschlossen.
- (3) Der Auftraggeber stimmt dem Einsatz (Auslagerung, Wechsel) zur Vertragsdurchführung als Unterauftragnehmer in den in 4 (2) genannten Ländern von der in **Anlage 1** genannten Unternehmen zu.
- (4) Der Auftragnehmer darf Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher oder allgemeiner Genehmigung des Auftraggebers, welche auch in einem elektronischen Format erfolgen kann, beauftragen. Die Genehmigung der in diesem AVV gelisteten Unterauftragnehmer gilt hiermit als erteilt. Die Zustimmung für die Auslagerung auf Unterauftragnehmer oder den Wechsel bestehender Unterauftragnehmer gilt als erteilt, wenn
 - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit (2 Wochen vorab) schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.
- (5) Verweigert der Auftraggeber die Genehmigungserteilung und geht diese Verweigerung auch über den erfolglosen Ablauf einer zur Abhilfe bestimmten Frist hinaus, so steht beiden Vertragsparteien ein Kündigungsrecht aus wichtigem Grund gem. §314 BGB zu. Ein wichtiger Grund liegt vor, wenn dem kündigenden Teil unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zur vereinbarten Beendigung oder bis zum Ablauf einer Kündigungsfrist nicht zugemutet werden kann.

However, the contractor is obliged to enter into appropriate and lawful agreements, and take control measures, to guarantee data protection and data security for customer data in case of outsourced ancillary services.

- (2) The contractor will independently bind the sub-contractor to the obligations included in this DPA. The subcontract shall be in writing. The contractor remains responsible to the customer. Most sub-contractors tasked with service contract implementation are affiliated companies within the group of companies, with an equity stake of more than 50 %, or controlling stake (“group of companies” in terms of article 4 para. 19 GDPR). In addition, the companies of the group of companies have in turn entered into DPA.
- (3) For service contract execution, the customer agrees to the deployment (outsourcing, replacement) as subcontractors in the countries listed in 4 (2) of the companies mentioned in **Annex 1**.
- (4) The contractor may engage subcontractors only with the prior expressed written or general approval of the Customer, which may also be in an electronic format. The consent to the subcontractors listed in this DPA shall be deemed granted. The consent for outsourcing to subcontractors or the change of existing subcontractors shall be deemed to have been granted if
 - the contractor notifies the customer of such outsourcing to subcontractors a reasonable time (2 weeks in advance) in writing or in text form and
 - the customer does not object to the planned outsourcing in writing or in text form to the contractor by the time the data is transferred, and
 - a contractual agreement in accordance with Article 28 (2-4) of the GDPR is used as a basis.
- (5) If the customer refuses to grant the approval and if this refusal continues beyond the unsuccessful expiry of a period set for remedy, either party shall have an extraordinary termination right for an important reason in accordance to §314 BGB (German Civil Code). An important reason exists, if the terminating part cannot be expected to continue the contractual relationship until the agreed termination or until the expiry of a notice period, taking into account all circumstances of the individual case and weighing the interests of both parties.
- (6) The right to call in a suitable body for the settlement of disputes (e.g. arbitration tribunal) is reserved.

- (6) Das Recht zur Hinzunahme einer geeigneten Stelle zur Streitbeilegung (z. B. Schiedsgericht) wird vorbehalten.

9 Mitwirkungs- / Unterstützungspflichten zur Wahrnehmung der Rechte von betroffenen Personen

- (1) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 der DSGVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung („Vergessenwerden“); Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).
- (2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen, vorausgesetzt
 - a) der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und
 - b) der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten laut Vergütungsregelung
- (3) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer unterstützt den Auftraggeber bei der Bearbeitung dieser Art Anfragen im Rahmen der gesetzlichen Vorgaben. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.
- (4) Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich Auftraggeber und Auftragnehmer, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

10 Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten hinsichtlich datenschutzrechtlicher Bestimmungen feststellt.

9 Cooperation- / support obligations for the protection of the rights of affected persons

- (1) Regarding the type of processing, the contractor supports the customer with appropriate technical and organisational measures to meet his obligation to reply to requests for protection of the rights of the affected person listed in chapter 3 GDPR (consideration of rights regarding transparency; right of information; right of rectification; right to deletion (“right to be forgotten”); right to restriction of processing; right to disclosure in case of rectification and deletion, as well as restriction of processing; right to data portability; right to objection; rights in case of automated individual decisions).
- (2) In case of a claim against the customer by an affected person concerning possible claims under article 82 GDPR, the contractor undertakes to support the customer in the defence against the claim to the best of his ability, provided that
 - a) the customer has requested this in writing and
 - b) the customer reimburses the costs occasioned by such support to the contractor in terms of the compensation arrangement
- (3) If an affected person approaches the contractor with a request for correction, deletion or disclosure, the contractor shall refer without delay the affected person to the customer, inasmuch as an assignment to the customer is possibly based on the specifications of the affected person. The contractor supports the customer in handling such request as required by statutory provisions. The contractor is not liable if the request of the affected person has not been replied to at all, or in an appropriate and timely manner.
- (4) In case of a claim for damages by an affected person in terms of article 82 GDPR, the parties are obliged to provide one another with support and to contribute towards clarifying the underlying situation.

10 Customer obligations

- (1) The customer must fully inform the contractor without delay if they identify within order results any errors or irregularities with respect to data protection provisions.
- (2) The customer identifies to the order processor the contact person for data protection issues that may arise in the context of this DPA.

11 Support for customer performance of duty

- (2) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des AVVs anfallende Datenschutzfragen.

11 Unterstützung zur Pflichterfüllung des Auftraggebers

- (1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; vorherige Konsultation).
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Auftragnehmers enthalten oder nicht auf sein Fehlverhalten zurückzuführen sind, kann der Auftragnehmer zuvor einen Vergütungsanspruch geltend machen, dessen Abgeltung in einer gesonderten Vergütungsvereinbarung getroffen wird.

12 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, Überprüfungen durchzuführen oder durch zu benennende Prüfer durchführen zu lassen. Der Auftragnehmer ermöglicht Überprüfungen, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei.
- (2) Jede Form der Überprüfung, Besichtigung und Kontrolle beim Auftragnehmer bedarf grundsätzlich einer vorherigen rechtzeitigen Ankündigung durch den Auftraggeber. Der Aufwand für die Ausübung des Besichtigungs- und Kontrollrechts muss stets in einem angemessenen und für den Auftragnehmer zumutbaren Umfang bleiben.
- (3) Die Besichtigungs- und Kontrollrechte betreffen explizit nicht Bereiche, in denen Daten Dritter verarbeitet oder gespeichert werden.

Um das Recht auf Einsichtnahme in Bereiche zu ermöglichen, in denen sowohl Daten des Auftraggebers als auch Daten Dritter verarbeitet werden, muss vorab eine gesonderte Verschwiegenheitsvereinbarung (NDA) zwischen Auftragnehmer und Auftraggeber geschlossen werden. Darüber hinaus muss dem Auftragnehmer die Möglichkeit gegeben werden, den gesamten Besichtigungsbereich derart vorbereiten zu können, dass der Zugriff auf Daten Dritter in jeder Hinsicht ausgeschlossen werden kann.

- (4) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Artikel 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem

- (1) The contractor supports the customer in regard to the type of processing and the information at his disposal in compliance with the obligations listed in articles 32 to 36 GDPR (guarantee of security of processing; notification of supervisory authorities in case of violations of the protection of personal data; notification of the person affected by a violation of the protection of personal data; data protection impact assessment; prior consultation).
- (2) The contractor can make a prior claim for compensation with regard to support services that are not included in the performance specification of the contractor and that do no result from his misconduct; its settlement is agreed in a separate compensation agreement.

12 Monitoring rights of the customer

- (1) The customer is entitled to conduct inspections, or to instruct designated auditors to conduct them. The contractor enables inspections that are conducted by the customer, or by an auditor instructed by the customer, and contributes to their implementation.
- (2) Any kind of inspection, visit or monitoring of the contractor generally requires prior timely announcement by the customer. The efforts involved in the exercise of the inspection- and monitoring right must be limited to a scope that is acceptable to the contractor.
- (3) Areas where the data of third parties is processed are expressly excluded from inspection- and monitoring rights.

To enable the right to inspect areas in which both customer's and third-party data are being processed, a separate non-disclosure agreement (NDA) must be concluded in advance between the contractor and the customer. In addition, the contractor must be given the opportunity to prepare the entire inspection area in such a way that the possibility of accessing third-party data can be excluded in any way.

- (4) The contractor shall ensure that the customer can ensure himself of the contractor's compliance with his obligations in accordance with article 28 GDPR. The contractor undertakes to provide the customer with the necessary information upon request and, in particular, to provide evidence of the implementation of technical and organisational measures.
- (5) Proof of such measures that concern not only the order at hand can include:

Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

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

- die Einhaltung entsprechender genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- 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)

(6) Für die Ermöglichung von Kontrollen und die damit entstehenden Aufwände durch den Auftraggeber kann der Auftragnehmer zuvor einen Vergütungsanspruch vereinbaren.

Das Recht des Auftraggebers zur Durchführung von Kontrollen wird durch einen Vergütungsanspruch des Auftragnehmers nicht eingeschränkt. Auch die DSGVO sieht keine Unentgeltlichkeit von Kontrollen vor. Der Vergütungsanspruch seitens des Auftragnehmers besteht, wenn der Auftraggeber in überdurchschnittlichem oder unverhältnismäßigem Ausmaß (i. d. R. mehr als 1x pro Kalenderjahr) Kontrollen einfordert, oder Kontrollen einfordert die den regulären Betrieb des Auftragnehmers beeinflussen oder damit verbundene personelle oder sonstige Mehraufwände, auch von Dienstleistern des Auftragnehmers, verursachen.

13 Löschung und Rückgabe von personenbezogenen Daten

- (1) Soweit vom Leistungsumfang im Rahmen der DSGVO umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.
- (2) Gemäß Art. 28 DSGVO (3) g sind nach Wahl des Auftraggebers nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten entweder zu löschen oder zurückzugeben. Auf Grundlage der im Nutzungsbedingungen vereinbarten Leistungen ist eine Rückgabe der Daten im eigentlichen Sinne nicht möglich, da personenbezogene Daten nur elektronisch (digital) vorliegen und elektronisch (digital) verarbeitet werden. Aus diesem Grunde beschränkt sich das Wahlrecht des Auftraggebers auf die Löschung der personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen.

- compliance with relevant rules of conduct in terms of article 40 GDPR
- certification under an authorised certification scheme under article 42 GDPR
- current attestations or report extracts of independent entities (e.g. auditors, revision, data protection officer, IT security department, data protection auditors, quality auditors)
- an appropriate certification by IT security- or data protection audit (e.g. under BSI basic protection)

(6) For the facilitation of inspections and certification related expenditures to the customer, the contractor may agree in advance to a claim for compensation.

Customer's right to perform inspections shall not be restricted by any claim for compensation of the contractor. The GDPR also doesn't provide for controls to be free of charge. Contractor's claim for compensation shall exist if the customer requests above-average or disproportionate controls (usually more than once per calendar year), or if he demands controls that influence customer's regular operations or cause additional personnel or other expenses, including additional or other expenses of the contractor's service providers.

13 Deletion and return of personal data

- (1) Provided they fall within the scope of the GDPR, the deletion concept, right to being forgotten, rectification and disclosure are to be implemented immediately upon documented instruction from the customer.
- (2) According to article 28 para. 3 lit. g GDPR, all personal data must either be deleted or returned after completion of the processing services at the discretion of the client. Based on the scope of services agreed in the service contract, a return of data is not possible, since personal data is only available electronically (digitally) and is processed electronically (digitally). For this reason, the customer's right of choice is limited to the deletion of the personal data after completion of the processing services.

At the end of the service contract, the contractor will delete all personal data of the customer relating to the previous subject matter of contract, unless there is an obligation to store personal data in accordance with union law or the law of the member states (e.g. §257 HGB - retention of documents, retention periods). The customer receives a deletion proof of the data.

Zum Vertragsende löscht der Auftragnehmer somit sämtliche personenbezogenen Daten des Auftraggebers zum vorangegangenen Vertragsgegenstand, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z.B. §257 HGB - Aufbewahrung von Unterlagen, Aufbewahrungsfristen). Der Auftraggeber erhält einen Nachweis über die Löschung der Daten.

- (3) In besonderen, vom Auftraggeber und Auftragnehmer zu vereinbarenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Nutzungsbedingungen bereits vereinbart.
- (4) 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 und dies nicht zu einer inhaltlichen Umgestaltung führt.
- (5) Sicherheitskopien, die zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, werden für die Dauer von 14 Tagen vorgehalten und dann automatisch gelöscht.
- (6) Das Löschkonzept umfasst nicht die individuellen personenbezogenen Daten des Auftraggebers und solche Daten, deren Aufbewahrung im Hinblick auf die Einhaltung übergeordneter gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (7) 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.

14 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

- (1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses AVVs gesetzliche Pflichten gemäß Artikel 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artikel 38 und 39 DSGVO ausübt.
- (2) Dessen Kontaktdaten werden dem Auftraggeber auf Verlangen zum Zweck der direkten Kontaktaufnahme mitgeteilt, oder sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- (3) Auftraggeber und Auftragnehmer haften für Verstöße gemäß den Bestimmungen von Artikel 82 DSGVO.
- (4) In allen Fällen, in denen der Auftraggeber als für die Verarbeitung Verantwortlicher gemäß Art. 34 Abs. (1)

- (3) In specific cases that have to be agreed between the customer and the contractor, data will be stored or transferred. Remuneration and protective measures for this will be agreed separately, unless they have already been agreed in the service contract.
- (4) No copies or duplicates are to be created without the knowledge of the customer. Excluded from this are backup copies, insofar as they are necessary to guarantee proper data processing, and this does not lead to a modification of contents.
- (5) Backup copies required to ensure proper data processing are kept for a period of 14 days. Subsequently, they will be deleted automatically.
- (6) The deletion concept does not include individual personal data of the customer, or such data as is required for the compliance with superordinate statutory retention obligations.
- (7) The contractor shall retain documentation showing that data processing was performed properly beyond the end of the agreement and in accordance with the respective retention periods. Alternatively, they can be returned to the customer at the end of the agreement.

14 Controls and other obligations of the contractor

- (1) Beyond compliance with the stipulations of this DPA, the contractor is subject to statutory obligations according to articles 28 to 33 GDPR; in particular he guarantees the written instruction of a data protection officer, who carries out his activity in terms of articles 38 and 39 GDPR.
- (2) The contact details of the data protection officer are to be communicated to the customer upon request for the purpose of making direct contact, or they are to be displayed readily accessible on the homepage of the contractor.
- (3) The customer and the contractor shall be liable for infringements in accordance with the provisions of Article 82 GDPR.
- (4) In all cases in which the customer as data controller is obliged pursuant to Art. 34 (1) GDPR to inform a natural person immediately after becoming aware of a breach of the protection of their personal data, the contractor shall inform the customer and provide all relevant information about the affected person after becoming aware of the issue and immediately

15 Statutory disclosure, written form requirement, governing law

DSGVO verpflichtet ist, eine natürliche Person unverzüglich nach Bekanntwerden einer Verletzung des Schutzes ihrer personenbezogenen Daten zu informieren, hat der Auftragnehmer den Auftraggeber unverzüglich nach Bekanntwerden der Angelegenheit zu informieren und alle relevanten Informationen über die betroffene Person bereitzustellen.

15 Informationspflichten, Schriftformklausel, Rechtswahl

- (1) Für Änderungen und Ergänzungen sowie Nebenabreden zu diesem AVV ist Schriftform erforderlich; dies gilt auch für diese Schriftformklausel. Mündliche Vereinbarungen bestehen nicht.
- (2) Sollte eine Bestimmung dieses AVVs ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so werden die Wirksamkeit und Durchführbarkeit der übrigen Bestimmungen davon nicht berührt. Die Vertragsparteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch diejenige Bestimmung zu ersetzen, die dem von den Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt.
- (3) Die Vertragsparteien verpflichten sich, diesen AVV vertraulich zu behandeln und Dritten gegenüber Angaben dazu nur insoweit zu machen, als dies gesetzlich vorgeschrieben oder zur Förderung der Zusammenarbeit zwischen Auftraggeber und Auftragnehmer erforderlich ist. Die Vertragsparteien verpflichten sich, über sämtliche im Rahmen dieses AVVs bekannt gewordenen betrieblichen und geschäftlichen Tatsachen und Informationen auch nach Beendigung des Vertragsverhältnisses strengstes Stillschweigen zu bewahren.
- (4) Ausschließlicher Gerichtsstand für etwaige Streitigkeiten, die sich aus diesem AVV ergeben, ist Solingen, Deutschland.

16 Sonstige Vergütungsregelung

- (1) Für zusätzliche, nicht durch diesen AVV geregelte Aufwendungen durch den Auftragnehmer wird eine Vergütung entsprechend der jeweils gültigen Preisliste des Auftragnehmers vereinbart, sofern nicht im Nutzungsbedingungen anderweitige Preise vereinbart sind.

- (1) Written form is required for modifications and additions, as well as for ancillary agreements to this DPA; this includes this clause requiring written form. Verbal agreements are excluded.
- (2) If a provision of this DPA is or becomes wholly or partially void or unenforceable, the validity and enforceability of the remaining clauses shall not be affected. The parties shall undertake to replace the ineffective or unenforceable provision with a provision that comes as close as possible to achieving the economic purpose of the ineffective or unenforceable provision.
- (3) The contracting partners undertake to treat this DPA confidentially and to provide third parties with information about it to the extent that is required by law, or necessary for the furtherance of collaboration between customer and contractor. The contracting partners undertake to treat with strict confidentiality all operational and business details resulting from this DPA, even after the end of the contractual relationship.
- (4) The sole legal venue for possible disputes arising from this confidentiality obligation is Solingen, Germany.

16 Other compensation arrangement

- (1) If additional expenses caused by the contractor are not regulated by this DPA, the compensation shall be agreed in accordance with the contractor's current price list, unless other prices are agreed in the service contract.

Datum / Date

- gem. DSGVO Art. 28 Abs. ohne Unterschrift seitens Auftragnehmer

According to GDPR Art. 28 para. 9 without signature of the contractor

Auftragnehmer | contractor (cisbox)
Geschäftsführer | Managing directors

Auftraggeber (Kunde) | customer
Gesetzliche*r Vertreter*in | legal representative*s

Christof Majer

Name in Druckbuchstaben | Name in block letters

Name in Druckbuchstaben | Name in block letters

(nur notwendig, wenn handschriftlich unterschrieben wird | only necessary if handwritten signature is used)

Anlagen

Anlage 1: Unterauftragnehmer und Datenschutzbeauftragter

Anlage 2: Technisch-organisatorische Maßnahmen

Annexes

Annex 1: Subcontractors and data protection officer

Annex 2: Technical and organisational measures

1 Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten i. S. d. DSGVO verarbeiten (Unterauftragnehmer). Je nach Auftrag und Kunde kann es sich hierbei um eines oder mehrere der nachfolgenden Unternehmen handeln.

Bei den zur Vertragsdurchführung eingesetzten Unterauftragnehmern handelt es sich um Unternehmen der Unternehmensgruppe gemäß Art. 4 Abs. 19 DSGVO.

1. **cisbox Ltd**
311 Duong So 8, Ward 11
Go Vap District
Ho Chi Minh City, Vietnam
(Indexierung)
2. **cisbox Software Ltd**
311 Duong So 8, Ward 11
Go Vap District
Ho Chi Minh City, Vietnam
(Softwareentwicklung)

2 Datenschutzbeauftragter

SICDATA – Datenschutz | IT-Sicherheit
Herr Tobias Erdmann
Heiligenstock 34c
42697 Solingen, Deutschland
T. +49 212 659 85 – 0

1 Subcontractors

For the purpose of data processing on behalf of the customer, the contractor uses the services of third parties that process data on his behalf in terms of the GDPR (sub-contractors). Depending on the customer, this may include one or several of the below companies.

Sub-contractors tasked with the implementation of the agreement are affiliated companies within the group of companies in terms of article 4 para. 19 GDPR.

1. **cisbox Ltd**
311 Duong So 8, Ward 11
Go Vap District
Ho Chi Minh City, Vietnam
(Indexing)
2. **cisbox Software Ltd**
311 Duong So 8, Ward 11
Go Vap District
Ho Chi Minh City, Vietnam
(Software development)

2 Data protection officer

SICDATA – Data protection | IT security
Mr Tobias Erdmann
Heiligenstock 34c
42697 Solingen, Germany
T. +49 212 659 85 – 0

Auftragsverarbeitungsvertrag – Anlage 2

Data processing agreement – Annex 2

cisbox

Technisch-organisatorische Maßnahmen

1 Verantwortliche Stelle

Firma:	cisbox GmbH
Straße:	Brühler Straße 58
PLZ, Ort:	D-42657 Solingen - Deutschland
Telefon:	+49 212 2315 0
E-Mail:	datenschutz@cisbox.com
Web:	https://www.cisbox.com

2 Vertraulichkeit (Artikel 32 Absatz 1 lit. b DSGVO)

Zutrittskontrolle

Getroffene Maßnahmen zur Verwehrung des unbefugten Zutritts zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Technische Maßnahmen

- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem

Organisatorische Maßnahmen

- Schlüsselregelung / Schlüsselbuch

Zugangskontrolle

Getroffene Maßnahmen zur Verhinderung der unbefugten Nutzung der Datenverarbeitungssysteme.

Technische Maßnahmen

- Authentifikation mit Benutzer + Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von VPN-Technologie

Organisatorische Maßnahmen

- Benutzerberechtigungen verwalten
- Erstellen von Benutzerprofilen
- Passwortvergabe / Passwortregeln
- Schlüsselregelung / Schlüsselbuch

Technical and organisational measures

1 Responsible entity

Company:	cisbox GmbH
Street:	Brühler Straße 58
ZIP, City:	D-42657 Solingen - Germany
Phone:	+49 212 2315 0
Email:	dataprotection@cisbox.com
Web:	https://www.cisbox.com

2 Confidentiality (article 32 para. 1 lit. b GDPR)

Access control

Measures that prevent unauthorised persons from gaining access to the data processing systems used for processing or utilising personal data.

Technical measures

- Automatic access control system
- Chip card-/ transponder lock system
- Manual lock system

Organisational measures

- Key rules / key book

Access control

Measure taken to prevent unauthorised use of data processing systems.

Technical measures

- Authentication with username + password
- Use of anti-virus software
- Use of firewalls
- Use of VPN technology

Organisational measures

- Managing user authorisation
- Creation of user profiles
- Password assignment / password rules
- Key rules / key book

Zugriffskontrolle

Getroffene Maßnahmen, nach denen die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen

- Einsatz von Aktenvernichtern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen

- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
- Passwortrichtlinie inkl. Länge und Wechsel

Trennungsgebot

Getroffene Maßnahmen, damit zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen

- Physikalisch getrennte Speicherung auf gesonderten Systemen
- Trennung von Produktiv- und Testsystem

Organisatorische Maßnahmen

- Festlegung von Datenbankrechten
- Logische Mandantentrennung

Access control

Measures to ensure that persons entitled to use data processing systems have access only to the data subject to their access rights, and that personal data cannot be read, copied, modified or removed without authorisation while processing, using and after saving.

Technical measures

- Use of shredders
- Proper destruction of storage media (DIN 66399)
- Physical deletion of storage media before reuse
- Recording of access to applications, particularly during the entry, modification and deletion of data

Organisational measures

- Deployment of service providers for the destruction of files and data (if possible with certificate)
- Password policy incl. length and update

Separation rule

Measures to ensure that data collected for different purposes can be processed separately.

Technical measures

- Physically separate storage on separate systems
- Separation of productive systems and testing systems

Organisational measures

- Specification of databank privileges
- Logical customer separation

3 Integrität (Artikel 32 Absatz 1 lit. b DSGVO)

Weitergabekontrolle

Getroffene Maßnahmen zur Verhinderung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen

- E-Mail-Verschlüsselung

Organisatorische Maßnahmen

- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

Eingabekontrolle

Getroffene Maßnahmen zur Möglichkeit der nachträglichen Überprüfung und Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen

- Protokollierung der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

4 Verfügbarkeit und Belastbarkeit (Artikel 32 Absatz 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Getroffene Maßnahmen, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen.

Technische Maßnahmen

- Feuerlöschgeräte in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Unterbrechungsfreie Stromversorgung

Organisatorische Maßnahmen

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recoverykonzepts
- Serverräume nicht unter sanitären Anlagen

3 Integrity (article 32 para. 1 lit. b GDPR)

Data transfer monitoring

Measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transfer, its transport or when saving it on data carriers, and that it is possible to check and establish the recipients to which the transfer of data using data transfer systems is scheduled.

Technical measures

- Email encryption

Organisational measures

- Transfer of data in anonymous or pseudonymous form

Input control

Measures to ensure that it is possible to check and establish retroactively whether and who entered, modified or removed personal data from processing systems.

Technical measures

- Logging of entry, modification and deletion of data

Organisational measures

- Storage of forms from which data are received in automated processing
- Traceability of entry, modification and deletion of data by individual username (not user groups)

4 Availability and capacity (article 32 para. 1 lit. b GDPR)

Availability control

Measures to ensure that personal data is protected from accidental loss or destruction:

Technical measures

- Fire extinguishers in server rooms
- Protected power strips in server rooms
- Uninterrupted power supply

Organisational measures

- Storage of backups at a secure, external location
- Creation of a backup- & recovery concept
- Server rooms not below sanitary facilities

Auftragsverarbeitungsvertrag – Anlage 2

Data processing agreement – Annex 2

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 25 Absatz 1 und Artikel 32 Absatz 1 lit. d DSGVO)

Auftragskontrolle

Getroffene Maßnahmen zur Sicherstellung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen

-

Organisatorische Maßnahmen

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DSGVO
- Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit
- Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren

6 Weitere Maßnahmen

Getroffene Maßnahmen hinsichtlich Datenschutz-Management, Incident-Response-Management und Voreinstellungen

Technische Maßnahmen

Datenschutz-Management

- Einsatz von www.meinDatenschutz.de als Datenschutzmanagement-Lösung

Datenschutzfreundliche Voreinstellungen (gem. Art. 25 Abs. 2 DSGVO)

- Datenschutzfreundliche Voreinstellungen in allen Applikationen an sämtlichen technisch möglichen Stellen

Organisatorische Maßnahmen

Incident-Response-Management

- Datenschutz-Management
- Regelmäßige Datenschutzzschulungen der Mitarbeiter (zu Beginn der Tätigkeit und danach regelmäßig wiederkehrend)

5 Procedure for regular inspection, assessment and evaluation (article 25 para. 1 and article 32 para. 1 lit. d GDPR)

Order control

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed only in accordance with the instructions of the customer.

Technical measures

-

Organisational measures

- Strict selection criteria for contractors (in particular with regards to data security)
- Continuous monitoring of the contractor and its activities
- Written instructions to the contractor (e.g. in order processing agreement) within the meaning of Article 28 GDPR
- Contractor employees bound to confidentiality
- Prior assessment of security measures taken by the contractor, and related documentation
- Agree effective monitoring rights concerning the contractor

6 Further measures

Measures taken regarding data protection management, incident-response management and presets

Technical measures

Data protection management

- Deployment of www.meinDatenschutz.de as data protection management solution

Presets in support of data protection (according to article 25 para. 2 GDPR)

- Data protection-friendly presets in all applications at all technically possible places

Organisational measures

Incident-Response-Management

- Data protection management
- Regular data protection training of employees (at the beginning of activities, then in regular intervals)