VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG (ART. 28, 29 DS-GVO) / AGREEMENT ON DATA PROCESSING ON BEHALF OF A CONTROLLER (ARTICLES 28, 29 OF THE GDPR)

zwischen / between

Mustermann AG

Mustersysteme

Abt. Musterproduktion

Musterstrasse 12

D-00001 Musterort

(nachstehend der Auftraggeber / Verantwortliche genannt / called the „Client / Controller“ below)

08.09.2022

Contact

Martin Mustermann

mm

Tel.: 002

Fax: 003

mm@Mustermann.de

Page 1 of 9

Doc.No. 001

Cust.No. 0

Required parameters

1.	**Gegenstand und Dauer des Auftrags**	**Subject and duration of the mandate**
1.1.	Der Auftraggeber beauftragt den Auftragnehmer hiermit, in dessen Auftrag personenbezogene Daten zu verarbeiten, soweit dies erforderlich ist, um die Leistungen zu erbringen, die jeweils durch §2.8 unserer Allgemeinen Geschäftsbedingungen geregelt sind (nachfolgend "Vertragsverhältnis" genannt). Der Auftragnehmer ist dabei als Auftragsverarbeiter für den Auftraggeber tätig.	The Client herewith commissions the Contractor to process personal data on their behalf to the extent required to provide the services listed each in §2.8 of our Terms and Conditions. (hereinafter referred to as the 'Contractual Relationship'). In doing so, the Processor is acting on behalf of the Client.
1.2.	Diese Vereinbarung beginnt und endet automatisch mit dem jeweiligen Vertragsverhältnis gemäß Ziffer 1.1 und ersetzt sämtliche bisherigen Vereinbarungen der Parteien im Sinne der Auftragsverarbeitung.	This Agreement commences and ends automatically with the respective Contractual Relationship pursuant to para. 1.1 and replaces all previous agreements of the Parties in terms of data processing.
1.3.	Das Recht beider Parteien zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.	The right of termination of each Party for cause remains unaffected.

1.4. Vorbehaltlich der Regelungen des jeweiligen Vertragsverhältnisses (siehe oben Ziffer 1.1) ist für jede Kündigung die Textform erforderlich.

Subject to the provisions of the respective Contractual Relationship (see above, para. 1.1), text form is required for any notice of termination.

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

Nature and purpose of the processing, type of personal data and categories of data subjects

2.1. Der Auftrag erfasst alle Arten von Verarbeitungen im Sinne der Datenschutz-Grundverordnung (DS-GVO). Zweck der Verarbeitung ist die Erfüllung des Vertragsverhältnisses gemäß Ziffer 1.1.

The mandate includes all types of processing within the meaning of the General Data Protection Regulation (GDPR). The purpose of the processing is to provide performance under the Contractual Relationship pursuant to para. 1.1.

2.2. Der Auftraggeber entscheidet ausschließlich und in eigener Verantwortung, welche Arten von personenbezogenen Daten zu welchen Kategorien betroffener Personen er vom Auftragnehmer verarbeiten lässt. Die Verarbeitungen des Auftragnehmers erfassen alle Arten von personenbezogenen Daten zu allen Kategorien betroffener Personen, die der Auftraggeber dem Auftragnehmer zur Erfüllung des Vertragsverhältnisses (Ziffer 1.1) offenbart, zum Beispiel (aber nicht ausschließlich) Geräte- oder Nutzungsdaten zu verschiedenen IT-Geräten und deren Nutzern, Kontaktdaten von Nutzern und/oder Abrechnungsdaten; betroffen können zum Beispiel (aber nicht ausschließlich) die Nutzer von IT-Geräten sein, der Auftraggeber selbst bzw. dessen Mitarbeiter oder Vertragspartner.

The Client decides exclusively and at their own responsibility, which types of personal data of which categories of data subjects are to be processed by the Contractor. The Contractor shall process all types of personal data of all categories of data subjects disclosed by the Client to the Contractor to perform the Contractual Relationship (para. 1.1), for example (but not limited to), device or usage data for various IT devices and their users, contact data of users and/or billing data; affected data subjects may be (but not limited to): the users of IT devices, the Client and/or their employees or contracting partners.

3. Technische und organisatorische Maßnahmen

Technical and organizational measures

3.1. Der Auftragnehmer trifft alle technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gemäß der Anlage zu 3.1: Datenschutzkonzept „Technische und organisatorische Maßnahmen i.S.d. Art. 32 Abs. 1 DSGVO“.

The Contractor shall take all technical and organisation measures to ensure adequate protection of the data of the Client pursuant to Annex 3.1: Data Privacy Concept “Technical and organizational measures within the meaning of Art. 32 para. 1 GDPR”.

Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen nach Vertragsschluss bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Any change in the technical and organizational measures by the Contractor after conclusion of the Agreement remains reserved; the Contractor shall ensure, however, that at least the contractually agreed level of protection will be provided.

3.2. Der Auftraggeber hat sich vor Abschluss des Vertragsverhältnisses (siehe oben Ziffer 1.1) über die technischen und organisatorischen Maßnahmen des Auftragnehmers anhand der vom Auftragnehmer bereitgestellten Informationen gemäß der Anlage 3.1 sowie Ziffer 9 dieser Vereinbarung informiert und wird dies nach Vertragsschluss in regelmäßigen Abständen tun. Der Auftraggeber trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der vom Auftraggeber bestimmten, zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Prior to the establishment of the Contractual Relationship (see above, para. 1.1), the Client has verified the technical and organizational measures of the Contractor based on information provided by the Contractor pursuant to Annex 3.1, as well as para. 9 of this Agreement and will continue to do so at regular intervals after conclusion of this agreement. The Client is responsible for ensuring that the respectively applicable, contractually agreed technical and organizational measures offer an adequate protection level for the risks to which the data intended by the Client for processing by the Contractor are exposed.

3.3. Wenn der Auftraggeber nach Abschluss dieser Vereinbarung entscheidet, dass die bislang vorhandenen technischen und organisatorischen Maßnahmen des Auftragnehmers zum Schutz bestimmter personenbezogener Daten unter Berücksichtigung der Kriterien des Art. 32 Absatz (1) DS-GVO nicht ausreichen, wird er dem Auftragnehmer vor der Offenbarung dieser bestimmten Daten die zusätzlich erforderlichen Maßnahmen benennen und mit dem Auftragnehmer eine Vereinbarung dazu treffen, welche Vertragspartei welche Maßnahmen zu welchen Kosten veranlassen wird.

If, after conclusion of this Agreement, the Client decides that the currently existing technical and organizational measures of the Client are not adequate to protect certain personal data, having due regard to the criteria of article 32(1) GDPR, the Client shall identify the additionally required measures to the Contractor prior to disclosing these data and will conclude an agreement with Contractor to determine the measures to be taken and which Contracting Party shall be responsible for initiating them and for bearing the costs.

4. Ort der Verarbeitung

4.1. Der Auftragnehmer verarbeitet die vereinbarungsgegenständlichen Daten in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

Der Auftragnehmer ist nur dann befugt, die Daten in einen Staat außerhalb der Europäischen Union bzw. außerhalb des Europäischen Wirtschaftsraums (sogenanntes „Drittland“) zu verlagern, sofern hierfür das in der Datenschutz-Grundverordnung festgelegte Schutzniveau für die vertragsgegenständlichen Daten gemäß den Art. 44 ff. DS-GVO gewährleistet wird.

Place of processing

The Contractor shall process the data, which form the subject of this Agreement, in a Member State of the European Union or in any other Contracting State of the Agreement on the European Economic Area.

The Contractor is only authorised to transfer the data to a state outside the European Union or outside the European Economic Area (a 'Third Country'), if the level of protection required by the General Data Protection Regulation for the data, which form the subject of this Agreement, is ensured in accordance with articles 44 et seq. of the GDPR.

5. Berichtigung, Einschränkung und Löschung von Daten; Anfragen von betroffenen Personen

5.1. 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.

Rectification, restriction and erasure of data; enquiries of data subjects

The Contractor may not rectify, erase or restrict the data to be processed on behalf of the Client on its own authority, but only in accordance with documented instructions of the Client.

5.2. Ausschließlich der Auftraggeber ist dafür verantwortlich, Anfragen Betroffener zur Geltendmachung ihrer Rechte zu beantworten, etwa auf Auskunftserteilung, Berichtigung, Einschränkung oder Löschung. Der Auftragnehmer unterstützt den Auftraggeber bei der Umsetzung der Betroffenenrechte durch geeignete technische und organisatorische Maßnahmen.

Wenn der Auftraggeber das Ersuchen der betroffenen Person nicht, nicht richtig oder nicht fristgerecht beantwortet, haftet der Auftragnehmer nicht und der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter frei und ersetzt ihm etwaige Schäden und Aufwendungen. Dies gilt nicht, soweit die unterbliebene, fehlerhafte oder nicht fristgerechte Antwort des Auftraggebers an die betroffene Person auf einer unterlassenen, fehlerhaften oder verspäteten Information vom Auftragnehmer an den Auftraggeber beruht.

The Client is solely responsible for replying to enquiries of data subjects regarding the assertion of their rights, e.g. providing information upon enquiry, or rectification, restriction or erasure. As part of the Contractual Relationship, the Contractor shall provide the necessary functions to retrieve, rectify, restrict or erase data. The Contractor supports the client in realization of his rights by provision of technical and organizational measures.

The Contractor shall not be liable if the Client does not reply, or replies incorrectly or late to the request of the data subject, and the Client shall indemnify the Contractor for any claims of third parties and reimburse any damage and expenses. This shall not apply if the outstanding, incorrect or late reply of the Client to the data subject is caused by the fact that the Contractor has failed to provide, or has provided incorrect or late information to the Client.

5.3. Der Auftraggeber ist für die Datenportabilität in Bezug auf die betroffene Person verantwortlich.

The Client is responsible for the data portability in regard to the data subject.

6. Verantwortungsbereich des Auftragnehmers; Informationen bei der Verletzung des Schutzes personenbezogener Daten

Der Auftragnehmer setzt folgende Maßnahmen um:

6.1. Zur Wahrung der Vertraulichkeit gemäß den Art. 28 Absatz (3) Satz 2 lit. b, 29, 32 Absatz (4) DS-GVO wird der Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte einsetzen, die auf die Vertraulichkeit verpflichtet und mit den für sie relevanten Bestimmungen zum Datenschutz vertraut sind. 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.

6.2. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

6.3. Auf Anforderung weist der Auftragnehmer die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber nach Maßgabe der Ziffer 9 dieser Vereinbarung nach.

6.4. Für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers gemäß Art. 30 Absatz (1) DS-GVO ist ausschließlich der Auftraggeber verantwortlich; der Auftragnehmer unterstützt ihn dabei auf Anforderung durch Bereitstellung von Informationen, soweit dies die Verarbeitung personenbezogener Daten nach dieser Vereinbarung betrifft und vom Vertragsverhältnis gemäß Ziffer 1.1 erfasst ist.

6.5. Falls dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, informiert er den Auftraggeber unverzüglich. Dabei teilt der Auftragnehmer auch Kontaktdaten mit, unter denen sich der Auftraggeber nach zusätzlichen Informationen zur Verletzung erkundigen kann.

6.6. Der Auftragnehmer ist verpflichtet, mit dem Auftraggeber zusammenzuarbeiten, um sämtliche Informationen zu erheben, die erforderlich sind, um den bzw. die betroffenen Personen bzw. die zuständige Datenschutzbehörde korrekt und vollständig über die Verletzung zu informieren.

Sphere of responsibility of the Contractor; information in case of a personal data breach

The Contractor shall implement the following measures:

To maintain confidentiality pursuant to sentence 2 lit. (b) of Article 28(3) and Articles 29, 32(4) of the GDPR, the Contractor shall only use employees, who have committed themselves to confidentiality and are familiar with the provisions on data protection relevant for them, to perform the works. The Processor and any person under the Processor's control who has access to personal data may process such data exclusively in accordance with the instructions of the Client, including the powers granted in this Contract, unless they are legally obliged to process them.

The Client and the Contractor shall cooperate upon request with the supervisory authority in the performance of their responsibilities.

The Contractor shall inform the Client without undue delay about control activities and measures of the supervisory authority to the extent that they relate to this mandate.

Upon request, the Contractor shall provide proof of the adopted technical and organizational measures to the Client pursuant to para. 9 of this Agreement.

The Client shall be exclusively responsible for the compilation of the records of processing activities of the Client pursuant to Article 30(1) of the GDPR; the Contractor shall assist the Client by providing - upon request - information relating to the processing of personal data pursuant to this Agreement and covered by the Contractual Relationship pursuant to para. 1.1.

If the Contractor becomes aware of a personal data breach, the Contractor shall inform the Client without undue delay. At the same time, the Contractor shall also provide contact data, where the Client may obtain additional information about the breach.

The Contractor is obliged to cooperate with the Client to collect all information that is necessary to inform the data subject(s) and/or the competent data protection authority correctly and comprehensively about the breach.

6.7. Nach der Meldung einer Verletzung personenbezogener Daten durch den Auftragnehmer an den Auftraggeber entscheidet der Auftraggeber in alleiniger Verantwortung, ob die Voraussetzungen für eine Meldung an Behörden bzw. betroffene Personen vorliegen und nimmt die Meldungen in alleiniger Verantwortung vor.

After the Contractor has reported a personal data breach to the Client, the Client shall decide at their own responsibility, if the conditions for a report to the authorities and/or the data subjects apply and shall make the report at their own and sole responsibility.

7. Unterauftragsverhältnisse

Subcontractor relationships

7.1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, Unterauftragnehmer einzusetzen. Der Auftragnehmer ist dabei verpflichtet, den Unterauftragnehmer

The Client herewith grants the Contractor general authorisation for the use of Subcontractors. In doing so, the Contractor is obliged

a) unter Berücksichtigung seiner technischen und organisatorischen Maßnahmen zum Datenschutz sorgfältig auszuwählen und

a) to carefully select the Subcontractor with due regard to the Subcontractor's technical and organizational measures for data protection, and

b) durch schriftlichen oder elektronischen Vertrag zu beauftragen und

b) to commission the Subcontractor through an agreement in written or electronic form, and

c) in Bezug auf den Unterauftrag mindestens in demselben Umfang zur Erfüllung datenschutzrechtlicher Anforderungen zu verpflichten, wie dies in dieser Vereinbarung für den Auftragnehmer gilt.

c) to oblige the Subcontractors to commit themselves to complying with legal data protection requirements in terms of the Subcontract to at least the same extent, as applies to the Contractor in terms of this Agreement.

d) Sofern eine Einbeziehung von Unterauftragnehmern in Drittländern erfolgen soll, stellt der Auftragnehmer sicher, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau im Sinne der Art. 44 ff. DS-GVO gewährleistet ist, zum Beispiel durch Abschluss einer Vereinbarung gemäß den von der EU-Kommission genehmigten EU-Standardvertragsklauseln. Der Unterauftragnehmer muss einen Vertreter in der EU bestellt haben.

d) If Subcontractors in third countries are to be involved, the Contractor shall ensure that the respective Subcontractors warrant an adequate level of data protection within the meaning of Article 44 et seq. of the GDPR, for example, by concluding an agreement according to the standard EU contract terms approved by the EU Commission. The Subcontractor must have appointed a representative in the EU.

7.2. Die Parteien stellen fest, dass die Voraussetzungen gemäß Ziffer 8.1 für die Unterauftragsverhältnisse vorliegen, die zum Zeitpunkt des Abschlusses dieser Vereinbarung bereits bestehen und sich aus dem Vertragsverhältnis (Ziffer 1.1) ergeben.

Bevor der Auftragnehmer an den erteilten Unteraufträgen Änderungen vornimmt in Bezug auf die Hinzuziehung oder Ersetzung weiterer Unterauftragnehmer, teilt er dies dem Auftraggeber schriftlich oder in elektronischer Form mit.

Der Auftraggeber kann in Bezug auf den weiteren Unterauftragnehmer innerhalb einer Frist von 3 Arbeitstagen seit Erhalt der Information hierüber schriftlich vom Auftragnehmer Informationen dazu verlangen, wie der weitere Unterauftragnehmer, die ihm zu übertragenen Pflichten gemäß dieser Vereinbarung erfüllen und sicherstellen wird. Wenn der Auftraggeber dem Auftragnehmer innerhalb einer Frist von 7 Arbeitstagen seit Erhalt dieser weiteren Information schriftlich mitteilt, dass der weitere Unterauftragnehmer nach Beurteilung des Auftraggebers diese Pflichten nicht sicherstellen kann, werden die Vertragsparteien im Interesse einer gütlichen Einigung nach einer Lösung suchen. Falls eine einvernehmliche Lösung scheitert, ist der Auftragnehmer befugt, nach eigener Wahl entweder seine Leistungen ohne Hinzuziehung des weiteren Unterauftragnehmers fortzusetzen oder das jeweilige Vertragsverhältnis und diese Vereinbarung in Bezug auf das entsprechende Vertragsverhältnis mit dem Auftraggeber innerhalb einer Frist von 4 Wochen zu kündigen. Für die Kündigung gilt im Übrigen Ziffer 1.4 dieser Vereinbarung. Der Auftragnehmer ist insofern auch zu einer Teilkündigung befugt, wobei er lediglich die betroffenen Leistungsteile des Vertragsverhältnisses kündigen kann und die Leistung teilbar sein muss. Nach einer Kündigung reduziert sich die Vergütung des Auftragnehmers entsprechend.

The Parties determine that the prerequisites pursuant to para. 8.1 are satisfied for the sub-contractor relationships already existing at the time of conclusion of this Agreement and resulting from the Contractual Relationship (para. 1.1).

Before the Contractor makes any changes to the Subcontractor mandates regarding the involvement or replacement of additional Subcontractors, the Client shall be informed accordingly in written or electronic format.

In regard to the additional Subcontractor, the Client may request in writing - within 3 working days of being so informed - information from the Contractor on how the additional Subcontractor will perform and warrant compliance with the duties assigned to that Subcontractor pursuant to this Agreement. If the Client informs the Contractor within a period of 7 working days since receipt of this additional information in writing that the additional Subcontractor is - according to the assessment of the Client - not able to warrant compliance with these duties, the Contracting Parties shall seek an amicable solution. If the Parties fail to achieve an amicable solution, the Contractor shall be entitled - at their choice - to either continue with their performance without involving the additional Subcontractor or to terminate the respective Contractual Relationship and this Agreement in regard to the corresponding Contractual Relationship with the Client within a period of 4 weeks. In all other respects, para 1.4 of this Agreement applies to the termination. The Contractor shall also be entitled to terminate partially, in which case only the affected parts of the performance of the Contractual Relationship may be terminated, provided that the performance is divisible. The remuneration of the Contractor shall be reduced accordingly after such termination.

7.3. Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste.

A Subcontractor relationship for the purposes of these provisions does not exist if the Con-tractor commissions a third party to provide services deemed to be mere ancillary ser-vices. This includes, for example, postal and courier services, shipping services, cleaning services, telecommunications services without specific reference to services provided by the Contractor to the Client, or guard services.

8. Nachweismöglichkeiten; Inspektionen und behördliche Kontrollen

Demonstration capabilities; inspections and regulatory controls

8.1. Der Auftragnehmer weist dem Auftraggeber auf dessen Anfrage die Einhaltung der in dieser Vereinbarung geregelten Pflichten mit geeigneten Mitteln nach, wobei dem Auftragnehmer das Wahlrecht zwischen mehreren geeigneten Mitteln zusteht. Geeignet sind zum Beispiel

- eine Darstellung der aktuell getroffenen technischen und organisatorischen Maßnahmen über die Punkte gemäß der Anlage zu Ziffer 3.1 dieser Vereinbarung,
- Nachweise zur Durchführung von Selbstaudits

At the Client's request, the Contractor shall demonstrate to the latter compliance with the obligations regulated in this Agreement by appropriate means, in which case the Contractor may choose between various appropriate means. Appropriate means are, for example:

- an outline of the currently implemented technical and organizational measures about the issues stipulated in Annex to para 3.1.
- documented conduct of self-audits,

8.2. Die Nachweise gemäß Ziffer 9.1 sollen nach Möglichkeit Inspektionen (Vor-Ort-Kontrollen) beim Auftragnehmer vermeiden. Wenn im Einzelfall dennoch eine Inspektion beim Auftragnehmer erforderlich sein sollte, wird diese auf Kosten des Auftraggebers durch einen unabhängigen externen Prüfer / eine unabhängige externe Prüferin durchgeführt, den / die der Auftragnehmer benennt. Der Auftragnehmer darf nur solche Prüfer/Prüferinnen benennen, die gegenüber dem Auftraggeber ihre Unabhängigkeit vom Auftragnehmer versichert und sich zur Verschwiegenheit verpflichtet haben. Die Prüfung wird rechtzeitig mit angemessener Vorbereitungsfrist (bis zu 90 Tagen) abgestimmt und findet während der üblichen Geschäftszeiten des Auftragnehmers statt. Sie darf den Betriebsablauf des Auftragnehmers nicht beeinträchtigen. Den Prüfbericht des Prüfers/der Prüferin erhalten beide Parteien. Derartige Kontrollen sind grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Abweichende Regelungen können der jeweiligen Servicevereinbarung (Ziffer 1.1) entnommen werden.

For that matter, provision of the measures and certificates pursuant to para. 9.1, shall pre-vent on-site inspections (on-site controls) at the Contractor's premises as far as possible. If in individual cases, an inspection at the Contractor's premises is required, the inspection shall be conducted at the expense of the Client by an independent, external auditor designated by the Contractor. The Contractor may only designate auditors, who have assured the Client of their independence from the Contractor and have committed themselves to confidentiality. The date of the audit shall be agreed subject to an adequate preparation time (up to 90 days) and shall take place during the normal business hours of the Contractor. The audit may not impair the course of business of the Contractor. Both Parties shall receive a copy of the audit report. Such controls must generally be limited to one day per calendar year. Different regulations can be found in the respective service agreement (para 1.1).

8.3. Der Auftragnehmer hat in jedem Fall das Recht, die Duldung von Kontrollen und die Erteilung von Informationen insoweit und dann zu verweigern, wenn die Kontrolle bzw. Informationserteilung ein Risiko darstellen würde für die Sicherheit der Datenverarbeitungsanlagen oder der darauf befindlichen Daten des Auftragnehmers oder Dritter (zum Beispiel anderer Auftraggeber des Auftragnehmers).

The Contractor may in any event refuse to tolerate the controls or to comply with the obligation to provide information if and to the extent that the controls or the provision of information would present a risk for the security of the data processing systems or for the data of the Client or of third parties (e.g. other clients of the Contractor) on those systems.

8.4. Der Auftraggeber trägt neben den Kosten des Prüfers/der Prüferin die Aufwendungen des Auftragnehmers, die diesem im Rahmen der Inspektion entstehen; dies gilt auch für etwaige Prüfungen, die eine Datenschutz- oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers beim Auftragnehmer vornimmt. Dies gilt nicht, sofern der Auftragnehmer eine Pflichtverletzung in Bezug auf die Pflichten aus dieser Vereinbarung begangen hat und / oder ein Verstoß des Auftragnehmers gegen die Datenschutzverpflichtungen vorliegt.

In addition to the costs of the auditor, the Client shall bear the expenses of the Contractor incurred by the latter as part of the inspection; the same shall apply to any inspections conducted by a data protection authority or other public supervisory authority of the Client at the Contractor's premises. This clause shall not apply, if the Contractor is in breach with the Agreement and / or there is a data breach attributable to the Contractor.

8.5. Die Überprüfungen bei Unterauftragnehmern nimmt ausschließlich der Auftragnehmer bzw. ein vom Auftraggeber und Auftragnehmer gemeinsam Beauftragter vor. Sie werden dem Auftraggeber auf dessen Anforderung nachgewiesen. Sofern die Überprüfung eines Unterauftragnehmers auf Anforderung des Auftraggebers erfolgt, trägt der Auftraggeber die damit verbundenen Kosten, auch, soweit sie beim Unterauftragnehmer entstehen. Dies gilt nicht, sofern der Auftragnehmer bzw. der Unterauftragnehmer eine Pflichtverletzung in Bezug auf die Pflichten aus dieser Vereinbarung begangen hat und / oder ein Verstoß des Auftragnehmers bzw. Unterauftragnehmers gegen die Datenschutzverpflichtungen vorliegt. Die Prüfung findet höchstens einmal pro Kalenderjahr statt, wobei der Auftragnehmer den Zeitpunkt bestimmt.

Inspections at Subcontractors shall be performed exclusively by the Contractor or by a par-ty commissioned jointly by the Client and the Contractor. Proof of these inspections shall be provided to the Client at their request. If a Subcontractor is checked at the request of the Client, the Client shall bear the costs related to the inspection, even if the Subcontractor in-curs these costs. This clause shall not apply, if the Contractor or Subcontractor is in breach with the Agreement and / or there is a data breach attributable to the Contractor or Subcontractor. Such inspections shall take place not more than once per year, and the Contractor shall determine the date of the inspection.

9. Weisungsbefugnis des Auftraggebers

Client's authority to issue instructions

circulee GmbH
Karlplatz 7
10117 Berlin
Germany

9.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den Weisungen des Auftraggebers. Die Weisungen des Auftraggebers müssen sich im Rahmen der geltenden Datenschutzgesetze, dieser Vereinbarung und des Vertragsverhältnisses (Ziffer 1.1) halten.

Soweit die Weisungen des Auftraggebers nicht bereits in einem bestehenden Vertragsverhältnis (Ziffer 1.1) enthalten sind, erteilt er seine Weisungen ausschließlich durch die in Ziffer 10.3 benannten Weisungsberechtigten an die dort genannten Weisungsempfänger, und zwar schriftlich, in einem vom Auftragnehmer angebotenen elektronischen Format bzw. durch die im Vertragsverhältnis genannten Verfahren.

Falls der Auftragnehmer durch eine gesetzliche Vorschrift zu einer bestimmten Verarbeitung verpflichtet ist, zu welcher es keine Weisung des Auftraggebers gibt, teilt er dies dem Auftraggeber mit, sofern das betreffende Gesetz die Mitteilung nicht verbietet.

The Contractor shall process personal data only within the framework of the agreements concluded and in accordance with the instructions of the Client. The instructions of the Client must remain with the ambit of the applicable data protection laws, this Agreement and the Contractual Relationship (para. 1.1).

Unless the instructions of the Client already form part of an existing Contractual Relation-ship (para. 1.1), the Client shall issue their instructions only through the persons authorised to issue instructions named in para. 10.3 to the recipients of instructions named there, in writing, in an electronic format offered by the Contractor and/or in the manner indicated by the Contractual Relationship.

If the Contractor is obliged by law to process data according to a certain method for which the Client has not issued any instructions, the Contractor shall inform the Client according-ly, unless the notification of the Client is prohibited by the relevant laws.

9.2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung könnte gegen Datenschutzvorschriften verstoßen. Die Parteien sind sich einig, dass der Auftragnehmer in diesem Zusammenhang auf die Richtigkeit und Vollständigkeit der Informationen des Auftraggebers angewiesen ist.

The Contractor shall inform the Client without undue delay if Contractor believes that an instruction may violate data protection laws. The Parties agree that the Contractor depends in this regard on the accuracy and integrity of the data of the Client.

9.3. Der Auftraggeber ist dafür verantwortlich, die für ihn weisungsberechtigten Personen durch die Nutzung der hierfür vom Auftragnehmer bereitgestellten Funktionalitäten zu definieren.

The Client shall be responsible for defining the persons authorised to issue instructions on behalf of the Client by using the functions provided by the Contractor for this purpose

10. Löschung und Rückgabe von personenbezogenen Daten; Vertraulichkeit auch nach Vertragsende

Erasure and return of personal data; confidentiality also beyond the term of the Agreement

10.1. Im Falle einer Verpflichtung zur Datenlöschung gewährleistet der Aufragnehmer eine datenschutzgerechte Löschung der vertragsgegenständlichen personenbezogenen Daten nach dem Stand der Technik.

In the event of an obligation to erase date, the Contractor shall ensure state-of-the-art data protection-compliant erasure of the personal data that form the subject of this Agreement.

10.2. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Copies or duplicates shall not be created without knowledge of the Client. This excludes backups, if they are necessary to ensure proper data processing, as well as data that are required in order to comply with legal retention requirements.

10.3. Während des Vertragsverhältnisses und bis zu einer Dauer von 30 Tagen danach stellt der Auftragnehmer Funktionen bereit zur Exportierung der vereinbarungsgegenständlichen Daten in dem von ihm angebotenen Standardformat. Der Auftraggeber weist den Auftragnehmer hiermit an, die vereinbarungsgegenständlichen Daten nach Ablauf dieser Frist zu löschen, sofern die Löschung nicht bereits Gegenstand des Vertragsverhältnisses gemäß Ziffer 1.1 ist.

During the term of the Contractual Relationship and for a period of up to 30 days following the end of such Contractual Relationship the Contractor shall provide features for exporting the data, which form the subject of this Agreement, in the standard format offered by the Contractor. The Client hereby instructs the Contractor to delete the data which form the subject of this Agreement, upon expiry of the aforementioned period, if such deletion / data erasure is not already subject of the Contractual Relationship pursuant to para. 1.1.

10.4. Der Auftragnehmer ist befugt, Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

Documentation that serves as proof of proper and contract-compliant data processing must be kept by the Contractor in accordance with the respective retention periods beyond the term of the Agreement.

10.5. Der Auftragnehmer ist verpflichtet, während und auch über das Ende des Vertrags hinaus die Vertraulichkeit aller vertragsgegenständlichen Informationen, Unterlagen und elektronischen Daten zu gewährleisten, soweit diese nicht auftragsgemäß vernichtet oder an den Auftraggeber zurückgegeben sind.

The Contractor is obliged - during as well as beyond the term of the Agreement - to ensure the confidentiality of all information, records and electronic data that form the subject of this Agreement if they are not destroyed in accordance with the provisions of the commission or returned to the Client.

11. Vergütung

Remuneration

11.1. Sofern die Maßnahmen des Auftragnehmers gemäß dieser Vereinbarung nicht ausdrücklich vom jeweiligen Vertragsverhältnis (siehe oben Ziffer 1.1) und der dort geregelten Vergütung erfasst sind, sind sie zu den aktuell geltenden Preisen des Auftragnehmers gesondert zu vergüten.

If the measures undertaken by the Contractor in terms of this Agreement are not expressly covered by the respective Contractual Relationship (see above, para. 1.1) and the remuneration stipulated there, they shall be remunerated additionally at the currently applicable prices of the Contractor.

12. Haftung

Liability

12.1. Es gelten die gesetzlichen Haftungsregelungen gem. Art. 82 DSGVO. Etwaige Haftungsbegrenzungen zwischen den Parteien (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung.

The legal liability provisions according to Art. 82 GDPR. Any limitation of liability between the parties (e.g. in the main contract) do not apply in this regard.

13. Wirksamwerden des Vertrags und Schlussbestimmungen

Effectiveness of the Agreement and final provisions

13.1. Die Vereinbarung wird wirksam, wenn sie vom Auftraggeber durch Setzen des entsprechenden Hakens während der Kontoerstellung akzeptiert wird. Der Auftraggeber verzichtet auf den Zugang der Annahmeerklärung des Auftragnehmers gemäß §151 Satz 1 BGB, wobei der Auftraggeber nicht befugt ist, Änderungen vorzunehmen an dem Vereinbarungstext, den er vom Auftragnehmer erhalten hat.

This agreement shall take effect when the Contractor accepts by checking the appropriate box during account creation. This Agreement shall take effect when the Contractor receives the original copy signed by the Client. The Client waives the right to a notice of acceptance by the Contractor pursuant to sentence 1 of section 151 of the German Civil Code [BGB], subject to the proviso that the Client is not authorised to make any changes to the text of the agreement received from the Contractor.

13.2. Für diese Vereinbarung gilt deutsches Recht.

This Agreement is governed by German law.

13.3. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

Any amendments and addenda to this Agreement must be done in writing. The same applies to any waiver of the written form requirement.

13.4. Für etwaige Streitigkeiten zwischen den Parteien ist das Landgericht Frankfurt am Main zuständig. Nach Wahl des Auftragnehmers kann auch das für deren Sitz zuständige Gericht oder die für IT-Sachen zuständige Kammer beim Landgericht Stuttgart angerufen werden.

The Regional Court [Landgericht] Frankfurt am Main is competent for any disputes be-tween the Parties. At the choice of the Contractor, a lawsuit may also be filed at the court competent for their registered office, or the Chamber competent for IT-related disputes at the Regional Court [Landgericht] Stuttgart.

Englische Übersetzung nur für Informationszwecke. Rechtsverbindlich ist ausschließlich die deutsche Version.

English version for information purposes only. Legally binding is only the German version.

circulee GmbH
Karlplatz 7
10117 Berlin
Germany

Circulee GmbH

Technische und organisatorische Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO

Stand: April 2022

Autor: Michael Heitele

Inhaltsverzeichnis

1 Einleitung

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

Gesetzlich geregelt sind die Anforderungen an die Datensicherheit in Art. 32 Abs. 1 DSGVO. Diese Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Das Gesetz nennt verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

(1) Vertraulichkeit

(2) Integrität

(3) Verfügbarkeit und Belastbarkeit

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(5) Pseudonymisierung und Verschlüsselung

Diese Maßnahmen stellen wir in der Folge vor, um Art. 28 Abs. 3 lit. c) DSGVO nachzukommen.

2 Organisatorisches

Die Circulee GmbH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus sowie der schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO verpflichtet.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung etwaiger Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit nicht detailliert veröffentlich werden.

3 Datenschutz-Management

Maßnahmen, die gewährleisten, dass personenbezogene Daten und Personen, die mit diesen arbeiten, organisatorisch auf den Umgang hingewiesen bzw. verpflichtet wurden.

Folgende Maßnahmen wurden im Unternehmen getroffen:

- Die Rollen DSKO, (e)DSB im Bereich Datenschutz sind benannt und über den Umfang ihrer jeweiligen Aufgaben informiert.
- Die Fachkunde des (e)DSBs wird sichergestellt.
- Es existiert ein on-boarding Prozess für neue Beschäftigte in dem Datenschutzthemen berücksichtigt werden und die Vergabe der Rechte durch die IT-Abteilung geregelt ist.
- Alle Beschäftigten haben eine Verpflichtung zur Einhaltung der Vertraulichkeit unterschrieben
- Alle neuen Beschäftigten erhalten bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz. Des Weiteren sind die Beschäftigten auf das Datengeheimnis verpflichtet worden.

- Die Beschäftigten werden regelmäßig durch Datenschutzschulungen/Awarenessmaßnahmen auf datenschutzgerechtes Verhalten geschult.
- Es existiert ein off-boarding Prozess zum Umgang mit ausscheidenden Beschäftigten und dem Entzug der erteilten Rechte/Betriebsmittel.

4 Schutzmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der Circulee GmbH betrieben werden.

4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (bspw. automatisches Zutrittskontrollsystem, manuelles Schließsystem, Videoüberwachung, Wachpersonal etc.).

Das Unternehmen setzt unterschiedliche physische Zutrittsbeschränkungen ein. Die eingesetzten Zutrittsbeschränkungen verhindern den Zutritt für Unbefugte zu den Geschäftsräumen sowie zum Serverraum/Rechenzentrum. Es werden folgende Zutrittsbeschränkungen eingesetzt:

- Es existiert eine Besucherverwaltung und alle Besucher des Unternehmens müssen sich am zentralen Empfang anmelden und dürfen die nicht-öffentlichen Bereiche nur in Begleitung betreten. Zusätzlich findet eine Erfassung der Besucher im Besucherbuch statt.
- Das Unternehmen setzt ein automatisches Zugangskontrollsystem ein, die berechtigten Personen verwenden zur Verifizierung Chipkarten / Token.
- Im Unternehmen werden Sicherheitsschlösser eingesetzt.
- Es existiert eine dokumentierte Schlüsselvergabe für die Schlüssel / Token / Chipkarten.
- Das Unternehmen hat einen Pförtner / eine Personenkontrolle, welche alle Besucher kontrolliert und registriert.
- Die Verteilerräume oder -bereiche (Gebäudetechnik) sind gegen unbefugten Zutritt gesichert.
- Es kommen einbruchhemmende Maßnahmen zum Einsatz (wie z.B. Sicherheitsfenster; Absicherung von Gebäudeschächten etc.).
- Es sind Sicherungsmaßnahmen gegen Überfälle im Einsatz (bspw. Gegensprechanlagen, elektrische Türöffner).
- Der Gebäudekomplex ist außerhalb der Geschäftszeiten geschlossen und kann nur von berechtigten Personen manuell geöffnet werden.
- Die Büroräume des Unternehmens sind separat gesichert über ein elektronisches Sicherheitsschloss / manuelles Schließsystem.
- Entsprechende Regelungen für den Zutritt von externen Personen (Wartungsdienst; Reinigungsdienst; Besucher) sind implementiert.

4.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (bspw. Maßnahmen zur Authentifikation, VPN-Verbindungen)

- Der Zugang zu den EDV-Systemen ist nur mit individuellen Benutzernamen und Kennwörtern möglich.

- Der Zugang zu den EDV-Systemen ist nur den Beschäftigten des Unternehmens möglich, welche hierfür die Zugangsberechtigung erhalten haben.
- erfolgt nach diesem definierten Prozess.
- Es erfolgt eine Protokollierung der Benutzeranmeldungen und des jeweiligen Zeitpunktes der Anmeldung.
- Es gibt für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen.
- Es werden Initialpasswörter verwendet und eine Änderung wird systemseitig bei der ersten Anmeldung erzwungen. Zusätzlich werden die Beschäftigten regelmäßig aufgefordert ihr Passwort zu ändern. Die fehlerhaften Passworteingaben werden protokolliert.
- Im Unternehmen erfolgt die Zuordnung von Benutzerprofilen zu den jeweiligen IT-Systemen.
- Im Unternehmen werden auf allen IT-Systemen Anti-Viren-Lösungen eingesetzt.
- Alle Geräte werden von der IT-Abteilung mit einer automatischen Bildschirmsperre (passwortgeschützt) zur Verfügung gestellt.
- Das Unternehmen schützt die IT-Infrastruktur durch Software- und Hardware-Firewalls.
- Die Authentifikation erfolgt mit Benutzername / Passwort.
- Die IT-Abteilung aktiviert die Verschlüsselung von Smartphone-Inhalten.
- Die IT-Abteilung aktiviert die Verschlüsselung von Datenträgern in Laptops / Notebooks.
- Es findet eine Reduktion zugriffberechtigter Personen auf ein Minimum statt.
- Die IT-Abteilung setzt ein Netzwerkmonitoring mit Alarmierung ein.
- Es wird ein separates Gäste-WLAN eingesetzt, so dass ein Zugang über dieses zum Firmennetzwerk nicht möglich ist.

4.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (bspw. automatische Prüfung der Zugriffsberechtigung mittels Passwort, differenzierte Zugriffsberechtigungen auf Anwendungsprogramme).

- Es existiert ein Rollen- und Berechtigungskonzept; die Berechtigungsprüfungen erfolgen auf Basis dieses Konzeptes.
- Es existiert eine im Berechtigungskonzept umgesetzte Trennung von Abrechnungs- und Kundenstammdaten.
- Die Berechtigungsvergabe basiert auf dem «need-to-know-Prinzip»
- Es existiert eine Anweisung an die Benutzer, wie mit den DV-Systemen bei Verlassen des Arbeitsplatzes (Sperren) umzugehen ist.
- Personenbezogene Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden.
- Eine Verwendung fortlaufend aktualisierter Virenschutzsoftware ist technisch durch die IT-Abteilung sichergestellt.
- Eingehender E-Mail-Verkehr wird durch ein zentrales Virenschutz- und Spamfiltersystem auf Viren und Spam überprüft.
- Es existiert eine Passwortrichtlinie, welche die aktuellen Empfehlungen des BSI berücksichtigt. Die Mindestkriterien sind systemseitig festgelegt.
- Auf den IT-Systemen findet eine Protokollierung von Datenänderungen statt.
- Das Unternehmen setzt eine Datenträgerverwaltung/ein Datenträgermanagement ein.
- Es ist ein softwareseitiger Ausschluss (Berechtigungskonzept) etabliert.
- Die Zugriffsmöglichkeiten der Benutzer sind auf den benötigten Umfang eingeschränkt.

- Es sind restriktive Zugriffsberechtigung/projektbezogene Zugänge etabliert.
- Es existiert ein abgestimmtes Berechtigungsvergabeverfahren.
- Es existieren abgestufte Zugriffsrechte mit Logging/Protokollierung.
- Es existiert eine Anweisung an die Mitarbeiter, wie mit nicht mehr benötigten Datenträgern (Papierform) umzugehen ist.
- Es existiert eine Anweisung über die Entsorgung von Geräten inkl. Speichermedien.

4.1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (bspw. Trennung Test- und Produktivumgebung, Trennung Managementnetz von Produktionsnetz, logische Trennung etc.).

- Das Unternehmen setzt ein Test- und Freigabeverfahren für Softwareprodukte ein.
- Im Unternehmen erfolgt die Trennung der Produktiv- von der Test- und Entwicklungsumgebung.
- Das Managementnetz ist vom Produktionsnetz getrennt.
- Die Entwicklungs- und Produktionsprogramme sind voneinander getrennt.
- Es existiert ein Änderungsmanagement mit differenziertem Freigabeverfahren.
- Es ist ein softwareseitiger Ausschluss (Mandantentrennung) etabliert.

4.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

4.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, 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 (bspw. Vernichtung, Löschung und Verschlüsselung von Datenträgern, VPN-Verschlüsselung, Hardwareverschlüsselung).

- Bei der Weitergabe von Daten werden nur freigegebene Verschlüsselungslösungen bei Übertragungen eingesetzt.
- Der Zugriff auf die Daten und Dateien über das Web erfolgt über eine SSL-verschlüsselte Verbindung.
- Regelung des Systemkommunikationsverkehrs (zentrale Firewall, exklusive WAN-Verbindungen (Wide Area Network) mit Zugriffkontrollen), Protokollierung (Userauthentifizierung, Zeitpunkt).
- Im Unternehmen existiert ein Verbot für den physischen Versand von Datenträgern.
- Alle Datenträger werden von der IT-Abteilung verschlüsselt.
- Der Aufbau der Transportverbindung findet nur zwischen definierten und durch Zertifikate gesicherten Systemen statt.
- Es ist ein Verbot für den Einsatz privater Datenträger vorhanden und wird technisch erzwungen.
- Die Beschäftigten können Dienste nur nutzen, die von der IT freigegebenen wurden.
- Es findet eine kontrollierte Vernichtung von Datenträgern und Papierdokumenten nach DIN 66399 statt.
- Es gibt eine vorgegebene Datenträgerverwaltung mit Bestandsüberwachung/ -kontrolle (Vollständigkeits- und Richtigkeitsprüfung). Des Weiteren existiert ein gesicherter Eingang für An- und Ablieferung.

4.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (bspw. Benutzerprofile, Protokollierung eingegebener Daten (Verarbeitungsprotokoll), gescheiterte Anmeldeversuche, administrative Tätigkeiten über ein Ticketsystem).

- Im Unternehmen werden systemseitige Plausibilitätskontrollen umgesetzt.
- Im Bedarfsfall kann nachträglich festgestellt werden, ob und von wem Kundenstammdaten in DV-Systeme eingegeben, verändert oder entfernt worden sind (Protokollierung).
- Alle Beschäftigten haben auf deren Berechtigungsumfang angepasste Benutzerprofile.
- Im Unternehmen erfolgt eine Protokollierung der eingegebenen Daten (Verarbeitungsprotokoll).
- In den EDV-Systemen sind Benutzeridentifikationen etabliert.
- Es findet eine Firewall-Protokollierung (TCP/IP) statt.
- Die Systeme sind so konfiguriert, dass eine Protokollierung der gescheiterten Anmeldeversuche stattfindet.
- Die administrativen Tätigkeiten werden protokolliert.
- Es existiert ein zentraler Log-Server.
- Es findet eine Protokollierung der Eingabe, Änderung und Löschung von Daten statt.
- Im Active Directory ist die Protokollierung der Benutzer aktiviert.
- Die kompletten protokollierten Daten sind gegen unbefugte Einsicht und/oder Manipulation gesichert.

4.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (bspw. USV und Notstromaggregat, Alarmanlage, redundante Datenspeicherung (RAID-Festplattensysteme), Firewalls, Virenschutzprogramme, mehrfache inkrementelle Datenbank- und Systembackups, Datensicherungskonzepte).

Die Circulee GmbH gewährleistet die Verfügbarkeit der Daten, sowie den Schutz gegen (zufällige) Zerstörung über die Inanspruchnahme der IT-Infrastruktur der Microsoft Azure-Umgebung. Gleiches gilt auch für die rasche Wiederherstellbarkeit.

Hierbei werden die Daten in europäischen Rechenzentren von Microsoft Azure gespeichert und unterliegen dort den zwischen Circulee GmbH und Microsoft vereinbarten Sicherheitsanforderungen. Die von Microsoft implementierten Maßnahmen können hier eingesehen werden:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-soc-2

4.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

4.4.1 Datenschutz-Management

Die Circulee GmbH betreibt ein Datenschutzmanagement-System (DSMS) nach den Vorgaben des Art. 5 Abs. 2 DSGVO. Es orientiert sich an dem PDCA-Zyklus und unterliegt damit einer dauerhaften Wirksamkeitsüberwachung.

4.4.2 Incident-Response-Management

Ein prozessualisierter Umgang mit Sicherheitsvorfällen ist implementiert. Im Falle eines Vorfalls informieren die Mitarbeiter die IT bzw. ihren Vorgesetzten unverzüglich. Im Anschluss erfolgt die Abstimmung mit dem Datenschutzbeauftragten. Die Bearbeitung von Vorfällen ist durch entsprechende Vertretungsregelungen sichergestellt.

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

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftstätigkeiten zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können.

4.4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (bspw. Verpflichtung auf die Vertraulichkeit bzw. Datengeheimnis, insbesondere der IT-Administratoren, Vertrag zur Auftragsverarbeitung nach Vorgabe des Art. 28 DSGVO, Sperrung der Zugriffe nach außen bspw. bei Fernwartung durch Externe, Vergabe restriktiver Zugriffsberechtigungen, Einbindung des Datenschutzbeauftragten/Informationssicherheitsbeauftragten etc.).

Voraussetzungen für das Eingehen eines Unterauftragsverhältnisses:

- Vertrag zur Auftragsdatenverarbeitung nach Vorgabe des Art. 28 Abs. 3 DSGVO.
- Deutsche Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsdatenverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

4.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

4.5.1 Pseudonymisierung

Sofern eine direkte Personenbeziehbarkeit nicht erforderlich ist, wird von der Pseudonymisierung Gebrauch gemacht, wenn dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (Datensparsamkeit).

Zudem werden Maßnahmen zu Privacy by design und Privacy by default, inkl. entsprechenden Schulungsmaßnahmen im Produktbereich, nach den Grundsätzen der Datenvermeidung und Datensparsamkeit umgesetzt.

4.5.2 Verschlüsselung auf Dateiebene:

(Bspw. Verschlüsselung von vertraulichen Dokumenten, verschlüsselte Übertragungswege via VPA, Aufbau Transportverbindung nur zwischen definierten und durch Zertifikate gesicherten Systemen, Datenübertragung von der Website erfolgt über eine SSL-Verschlüsselung).

- Es werden Verschlüsselungstechnologien nach dem aktuellen Stand der Technik eingesetzt. Das bedeutet, es kommen TLS(SSL)-Verschlüsselungen, Hash-Verschlüsselungen etc. zum Einsatz.

4.5.3 Verschlüsselung auf Hardwareebene:

(Bspw. Verschlüsselung von Festplatten in Notebooks, passwortgeschützte Hardware etc.).

- Es werden Verschlüsselungstechnologien für die Hardwareebene nach dem aktuellen Stand der Technik eingesetzt (z.B. Bitlocker)
- Die Übermittlungswege werden gesamthaft dokumentiert.

5 Kooperation

Zur Einhaltung der datenschutzrechtlichen Vorgaben nach der DSGVO, arbeitet die Circulee GmbH mit der DDSK GmbH zusammen. Neben der Erstellung von Richtlinien und Handlungshilfen berät die DDSK GmbH die Circulee GmbH in allen Fragen rund um den Datenschutz und stellt mit Frau Irina Weiß die externe Datenschutzbeauftragte nach Art. 37 DSGVO des Unternehmens.

DDSK GmbH

Irina Weiß

Dr. Klein-Straße 29, 88069 Tettnang

Tel. 07542 / 949 21 0

E-Mail: weiss@ddsk.de

Web: www.ddsk.de