| VEREINBARUNG AUFTRAGSVERARBEITUNG (AVV) | DATA PROCESSING AGREEMENT (DPA) |
|---|---|
| **gemäß der EU-Standardvertragsklauseln aus dem Durchführungsbeschluss 2021/915 der Kommission vom 4. Juni 2021** | **Pursuant to the EU standard contractual clauses from Commission Implementing Decision 2021/915 of June 4, 2021** |
| ***Erläuterung:***<br><br>*Es handelt sich bei dieser Auftragsverarbeitungsvereinbarung (gemäß Durchführungsbeschluss 2021/915) um die Standardvertragsklauseln der EU-Kommission für Auftragsverarbeitungen innerhalb der EU und damit quasi um einen Mustervertrag für Auftragsverarbeitungsvereinbarungen gemäß Art. 28 DSGVO.*<br><br>*Es handelt sich NICHT um die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (gemäß Durchführungsbeschluss 2021/914).*<br><br>*Wenn die EU-Kommission einen Mustervertrag zur Verfügung stellt, bietet es sich unseres Erachtens an, diesen auch zu verwenden, da die Verwendung des Mustervertrages beiden Parteien die Sicherheit gibt, eine Auftragsverarbeitungsvereinbarung abzuschließen, die den Anforderungen des Art. 28 DSGVO genügt, ohne einen Individualvertrag im Detail prüfen zu müssen.*<br><br>*Die Benennung der Parteien, die Beschreibung der Auftragsverarbeitung und der technischen und organisatorischen Maßnahmen und ggf. die Liste der Unterauftragsverarbeiter erfolgen in den Anhängen I bis IV.* | ***Explanatory note:***<br><br>*This data processing agreement (pursuant to Implementing Decision 2021/915) is the EU Commission's standard contractual clauses for processing operations within the EU and is therefore a quasi-model contract for processing agreements pursuant to Art. 28 GDPR.*<br><br>*It is NOT the standard contractual clauses for the transfer of personal data to third countries (pursuant to Implementing Decision 2021/914).*<br><br>*In our opinion, if the EU Commission provides a model contract, it is a good idea to use it as well, since the use of the model contract gives both parties the security of concluding a contract processing agreement that meets the requirements of Art. 28 GDPR without having to examine an individual contract in detail.*<br><br>*The naming of the parties, the description of the commissioned processing and the technical and organizational measures and, if applicable, the list of sub-processors are provided in Annexes I to IV.* |
| **ABSCHNITT I**<br><br>**Klausel 1: Zweck und Anwendungsbereich**<br><br>a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Art. 28 Abs. 3 und 4 DSGVO sichergestellt werden.<br><br>**b)** Die in **Anhang I** aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Art. 28 Abs. 3 und 4 DSGVO zu gewährleisten.<br><br>***c)*** Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß **Anhang II**.<br><br>***d)*** Die **Anhänge I bis IV** sind Bestandteil der Klauseln.<br><br>***e)*** Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der DSGVO unterliegt. | **SECTION I**<br><br>**Clause 1: Purpose and scope**<br><br>a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Art. 28(3) and (4) GDPR.<br><br>b) The controllers and processors listed in **Annex I** have agreed to these Clauses in order to ensure compliance with Art. 28(3) and (4) GDPR.<br><br>c) These Clauses apply to the processing of personal data as specified in **Annex II**.<br><br>d) **Annexes I to IV** are an integral part of the Clauses. |

***f)*** Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der DSGVO erfüllt werden

**Klausel 2: Unabänderbarkeit der Klauseln**

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

**Klausel 3: Auslegung**

a) Werden in diesen Klauseln die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

**Klausel 4: Vorrang**

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

**Klausel 5: Kopplungsklausel**

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of GDPR.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of GDPR.

**Clause 2: Invariability of the Clauses**

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects

**Clause 3: Interpretation**

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

**Clause 4: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 5: Docking clause**

a) Any entity that is not a Party to these Clauses may, with the agreement of all

Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

**ABSCHNITT II: PFLICHTEN DER PARTEIEN**

**Klausel 6: Beschreibung der Verarbeitung**

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in **Anhang II** aufgeführt.

**Klausel 7: Pflichten der Parteien**

**7.1. Weisungen**

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

**7.2. Zweckbindung**

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in **Anhang II** genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

**7.3. Dauer der Verarbeitung personenbezogener Daten**

Die Daten werden vom Auftragsverarbeiter nur für die in **Anhang II** angegebene Dauer verarbeitet.

**7.4. Sicherheit der Verarbeitung**

the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

**SECTION II: OBLIGATIONS OF THE PARTIES**

**Clause 6: Description of processing(s)**

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

**Clause7: Obligations of the Parties**

**7.1. Instructions**

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

**7.2. Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen

**7.5. Sensible Daten**

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

**7.6. Dokumentation und Einhaltung der Klauseln**

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung

processing, as set out in Annex II, unless it receives further instructions from the controller.

**7.3. Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in **Annex II.**

**7.4. Security of processing**

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or whether unintentional or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**7.5. Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply

| | |
|---|---|
| von Daten gemäß diesen Klauseln umgehend und in angemessener Weise. | specific restrictions and/or additional safeguards.<br><br>**7.6. Documentation and compliance** |



c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung

**7.7. Einsatz von Unterauftragsverarbeitern**

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen,

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

**7.7. Use of sub-processors**

a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben

**7.8. Internationale Datenübermittlungen**

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**7.8. International transfers**

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take

| | |
|---|---|
| stehen. | place in compliance with Chapter V of |

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Art. 46 Abs. 2 DSGVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

**Klausel 8: Unterstützung des Verantwortlichen**

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

**Clause 8: Assistance to the controller**

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects’ requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller’s instructions.

c) In addition to the processor’s obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a ‘data protection impact assessment’) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2) the obligation to consult the

| | |
|---|---|
| | competent supervisory |



2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Art. 32 DSGVO.

d) Die Parteien legen in **Anhang III** die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest

**Klausel 9: Meldung von Verletzungen des Schutzes personenbezogener Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Art. 33 und 34 DSGVO nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

**9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

4) the obligations in Art. 32 GDPR.

d) The Parties shall set out in **Annex III** the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

**Clause 9: Notification of personal data breach**

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Art. 33 and 34 GDPR, taking into account the nature of processing and the information available to the processor.

**9.1 Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Art. 33 (3) GDPR, shall be stated in the controller's notification, and must at least include:

1) the nature of the personal data including where possible, the

b) bei der Einholung der folgenden Informationen, die gemäß Art. 33 Abs. 3 DSGVO in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

c) Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt

d) bei der Einhaltung der Pflicht gemäß Art. 34 DSGVO, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat

**9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2) the likely consequences of the personal data breach;

3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

c) Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) in complying, pursuant to [OPTION 1] Article 34 of Regulation (EU) 2016/679 / [OPTION 2] Article 35 of Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

**9.2 Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Art. 33 und 34 DSGVO zu unterstützen.

**ABSCHNITT III: SCHLUSSBESTIMMUNGEN**

**Klausel 10: Verstöße gegen die Klauseln und Beendigung des Vertrags**

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Art. 33 and 34 GDPR.

**SECTION III: FINAL PROVISIONS**

**Clause 10: Non-compliance with the Clauses and termination**

a) Without prejudice to any provisions of GDPR, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

2) the processor is in substantial or persistent breach of these Clauses or its obligations under GDPR;

3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to GDPR.

| | |
|---|---|
| Verpflichtungen gemäß der DSGVO nicht erfüllt;<br><br>3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln oder der DSGVO zum Gegenstand hat, nicht nachkommt.<br><br>c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.<br><br>d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln. | c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.<br><br>d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses. |



## ANHANG I:
## LISTE DER PARTEIEN

## ANNEX I:
## LIST OF PARTIES

| **Verantwortlicher**<br>**Controller** | |
|---|---|
| Name:<br>Name: | *Auftraggeber, wie im Auftrag angegeben*<br>*Customer, as specified in the order* |
| Anschrift:<br>Address: | |
| Name, Funktion und Kontaktdaten der Kontaktperson:<br>Contact person's name, position and contact details: | |

ggf. Name und Kontaktdaten des Datenschutzbeauftragten:
name and contact details of the data protection officer (if any)

Datum und Unterschrift: Date and Signature:

Vertragsbestandteil durch Referenzierung im Auftrag Incorporated by reference in the order

| **Auftragsverarbeiter**<br>**Processor** | |
|---|---|
| Name:<br>Name: | Decify GmbH |
| Anschrift:<br>Address: | Agnes-Pockels-Bogen 1<br>80992 München |
| Name, Funktion und Kontaktdaten der Kontaktperson:<br>Contact person's name, position and contact details: | Laura Lehmann<br>Agnes-Pockels-Bogen 1<br>80992 München<br>office@tracify.ai |

ggf. Name und Kontaktdaten des Datenschutzbeauftragten:
name and contact details of the data protection officer (if any)

Agnes-Pockels-Bogen 1
80992 München
office@tracify.ai

Datum und Unterschrift:
Date and Signature:
Laura Lehmann

Vertragsbestandteil durch Referenzierung im Auftrag Incorporated by reference in the order

# ANHANG II:
# BESCHREIBUNG DER VERARBEITUNG

# ANNEX II:
# DESCRIPTION OF THE PROCESSING

**Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden: Categories of data subjects whose personal data is processed:**

Besucher*innen der Webseite/Webshops des Auftraggebers

Visitors to the Customer's website/webshops

**Kategorien personenbezogener Daten, die verarbeitet werden:**

**Categories of personal data processed:**

- Nutzungsdaten/Usage Data
- IP-Adresse/IP Address
- Bestellinformationen/Order Information
- Bestell-ID/Order-ID
- Kontaktdaten/Contact Data
- Browser- und Clientkonfiguration/Browser and Client Configuration

**Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:**

**Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

n/a

**Art der Verarbeitung:**

**Nature of the processing:**

Der Auftraggeber nutzt die Software Decify des Auftragnehmers für datenbasiertes Kundenverständnis. An den Auftragnehmer werden personenbezogene Daten übermittelt, damit der Auftragnehmer darauf aufbauend Auswertungen zur Verwendung der Webseite des Auftraggebers erstellen kann.

The Customer uses the Contractor's Decify software for data-based customer understanding. Personal data is transmitted to the Contractor so that the Contractor can use it to create evaluations on the use of the Customer's website.

**Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:**

**Purpose(s) for which the personal data is processed on behalf of the controller**

| |
|---|
| Erstellung von Auswertungen zur Nutzung und Verwendung der Webseite des Auftraggebers, um diese kontinuierlich den Anforderungen der Besucher anpassen und optimieren zu können.<br><br>Creation of evaluations on the use and utilization of the client's website in order to continuously adapt and optimize it to the requirements of the visitors. |
| **Dauer der Verarbeitung:**<br><br>**Duration of the processing** |
| Die Verarbeitung der personenbezogenen Daten im Rahmen des Auftragsverarbeitungsvertrags erfolgt konform mit den Anforderungen der Datenschutz-Grundverordnung (DSGVO). Hiermit wird festgelegt, dass die personenbezogenen Daten für eine Dauer von 24 Monaten ab dem Zeitpunkt der Datenerhebung gespeichert werden, sofern nicht eine anderslautende schriftliche Vereinbarung mit dem Kunden getroffen wurde. Diese Frist spiegelt unser Engagement wider, die Daten nicht länger als notwendig zu speichern und die Rechte der betroffenen Personen zu wahren. Jegliche Abweichung von dieser Speicherdauer wird individuell dokumentiert und ist Teil unserer maßgeschneiderten und datenschutzkonformen Verarbeitungsgrundsätze.<br><br>The processing of personal data within the framework of the data processing agreement complies with the requirements of the General Data Protection Regulation (GDPR). It is hereby stipulated that personal data will be stored for a period of 24 months from the time of data collection, unless a different written agreement has been made with the client. This period reflects our commitment to not retain data for longer than necessary and to protect the rights of the data subjects. Any deviation from this storage duration will be individually documented and forms part of our tailored and GDPR-compliant processing principles. |

**Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.**

**For processing by (sub-) processors, also specify subject matter, nature and duration of the processing**

## ANHANG III:
## TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

## ANNEX III:
## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

B

**1. Vertraulichkeit**

**1.1 Zutrittskontrolle**

Die Software wird bei Amazon Web Service EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg gehostet. Detaillierte Informationen zu den technischen und organisatorischen Maßnahmen im Rechenzentrum finden sich hier:

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Unsere Büroräume befinden sich in einem Bürohaus. Die Zugänge zum Bürohaus und auch zu den Büroräumen des Unternehmens sind Tag und Nacht verschlossen. Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Es kommt ein elektronisches Schließsystem zum Einsatz, das vom Vermieter verwaltet wird. Jeder Mieter des Bürohauses erhält zusätzlich Schlüssel zu den Büroräumen, die von der Personalabteilung verwaltet werden.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt. Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Der Empfang kann die Eingangstür einsehen und

**1. Confidentiality**

**1.1 Physical Access Control**

The Software is hosted at Amazon Web Service EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg. Detailed information on the technical and organizational measures in the data center can be found here:

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Our offices are located in an office building. The entrances to the office building and also to the company's offices are locked day and night. Only the landlord and the tenants of the office premises have access to the office building. An electronic locking system is used, which is managed by the landlord. Each tenant of the office building additionally receives keys to the office rooms, which are managed by the HR department.

Key allocation and key management is carried out in accordance with a defined process that regulates the granting or withdrawal of access authorizations for rooms both at the beginning of an employment relationship and at the end of an employment relationship.

Access authorizations are only granted to an employee if this has been requested by the respective supervisor and/or the HR department. The principle of necessity is taken

trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Die Eingänge und Fenster des Bürohauses und auch der Büroräume sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Unabhängig davon wird die Alarmanlage täglich jedoch stets am Abend automatisch aktiviert.

into account when issuing authorizations.

The receptionist may view the entrance door and shall ensure that each visitor reports to the receptionist.

Visitors are not permitted to move freely in the office space without an escort.



**1.2 Zugangskontrolle**

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Personalabteilung gestellt werden.

Der Auftragsverarbeiter verpflichtet sich, angemessene Maßnahmen zur Gewährleistung der Sicherheit von Passwörtern zu ergreifen. Dies umfasst die Implementierung einer Passwortsicherheitsrichtlinie, die Anforderungen an Passwortlänge, -komplexität und -erneuerung beinhaltet. Der Auftragsverarbeiter stellt sicher, dass Passwörter sicher gespeichert und vor unbefugtem Zugriff geschützt werden. Darüber hinaus wird der Auftragsverarbeiter regelmäßig überprüfen, ob die Passwortsicherheitsrichtlinien eingehalten werden, und sicherstellen, dass seine Mitarbeiter in bewährten Passwortpraktiken geschult sind. Die Zugriffsrechte auf personenbezogene Daten werden gemäß der erteilten Autorisierung verwaltet, und der Zugriff wird mittels geeigneter Authentifizierungsmethoden, einschließlich Passwörtern, geschützt.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

Remote-Zugriffe auf IT-Systeme erfolgen stets über verschlüsselte Verbindungen.

Auf den Servern ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

**1.3 Zugriffskontrolle**

Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet.

The entrances and windows of the office building and also of the office rooms are secured by an alarm system. This can be activated and deactivated manually. Independently of this, the alarm system is automatically activated daily, but always in the evening.

**1.2 System Access Control**

To gain access to IT systems, users must have the appropriate access authorization. These authorizations are granted by administrators but only when requested by the respective supervisor. The request can also be made through HR.

The processor is committed to taking reasonable measures to ensure password security. This includes implementing a password security policy that encompasses requirements for password length, complexity, and renewal. The processor ensures that

passwords are securely stored and protected from unauthorized access. Additionally, the processor will regularly check if password security policies are being followed and ensure that its employees are trained in best practices for passwords. Access to personal data is managed according to the given authorization, and access is protected using appropriate authentication methods, including passwords.

Passwords are generally stored in encrypted form. Remote access to IT systems is always via encrypted connections.

An Intrusion Prevention System is used on the servers. All server and client systems have antivirus software with daily signature updates. All servers are protected by firewalls, which are regularly maintained and updated with patches.

The access of servers and clients to the Internet and the access to these systems from the Internet are also secured by firewalls.

This ensures that only the ports required for communication are usable, with all others blocked.

All employees are instructed to lock their IT systems when they leave them.

**1.3 Data Access Control**

Authorizations for IT systems and applications are set up exclusively by administrators.

Authorizations are generally granted according to the need-to-know principle, so only those who maintain or work on the development of



Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei der Personalabteilung gestellt werden.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Alle Mitarbeitenden sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte.

Mitarbeitenden ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheitsupdates aktualisiert.

**1.4 Trennung**

Alle für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

**1.5 Pseudonymisierung & Verschlüsselung**

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

**2. Integrität**

**2.1 Eingabekontrolle**

Die Eingabe, Änderung und Löschung, insbesondere von personenbezogenen Daten, die im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Mitarbeitende sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

**2.2 Weitergabekontrolle**

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden verarbeitet werden, erfolgt jeweils nur in dem Umfang, in dem dies mit dem jeweiligen Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeitenden, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

data, databases, or applications are granted access rights.

Prerequisite is an authorization request for an employee by a supervisor. This request can also be made through HR. There is a role-based authorization concept that allows for differentiated assignment of access rights, ensuring employees receive access rights to applications and data based on their respective area of responsibility and, if necessary, on a project basis.

All employees are instructed to lock their IT

systems when they leave them. Employees are generally prohibited from installing unauthorized software on IT systems. All server and client systems are regularly updated with security patches.

**1.4 Separation**

All IT systems used for clients are multi-client capable. The separation of data from different clients is always guaranteed.

**1.5 Pseudonymization & Encryption**

Administrative access to server systems is always via encrypted connections.

**2. Integrity**

**2.1 Input Control**

The input, modification, and deletion of personal data processed on behalf of the controller are always logged. Employees are obliged to work with their own accounts at all times. User accounts may not be shared or used jointly.

**2.2 Transfer Control**

Personal data processed on behalf of customers is shared only to the extent necessary or agreed upon with the customer to provide contracted services.

All employees involved in customer projects are trained on the proper use of data and the modalities of data transfer. Employees are prohibited from using personal data carriers in connection with customer projects.

All employees are regularly trained on data protection topics and obligated to handle personal data confidentially.

**3. Availability and Resilience**

Data on server systems is backed up at least daily incrementally and weekly with a full backup.



Die Nutzung von privaten Datenträgern ist den Mitarbeitenden im Zusammenhang mit Kundenprojekten untersagt.

Alle Mitarbeitenden werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeitenden sind zudem auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

**3. Verfügbarkeit und Belastbarkeit**

Daten auf Serversystemen werden mindestens täglich inkrementell und wöchentlich voll gesichert.

Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es besteht ein Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

**4. Auftragskontrolle**

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts eine Vereinbarung Auftragsverarbeitung abgeschlossen. Auftragsverarbeiter werden initial und anschließend regelmäßig auditiert.

**5. Privacy by Design und Privacy by Default**

Der Auftragsverarbeiter verpflichtet sich, den Datenschutz durch technische und organisatorische Maßnahmen (Privacy by Design) sicherzustellen und datenschutzfreundliche Voreinstellungen (Privacy by Default) zu implementieren.

Diese Maßnahmen sollen gewährleisten, dass personenbezogene Daten auf ein notwendiges Minimum beschränkt sind und nur gemäß den Anweisungen des Verantwortlichen verarbeitet werden. Der Auftragsverarbeiter ist dafür verantwortlich, dass diese Prinzipien während des gesamten Entwicklungs- und Betriebsprozesses eingehalten werden. Der Verantwortliche behält sich das Recht vor, die umgesetzten Maßnahmen und Voreinstellungen regelmäßig zu überprüfen und bei Bedarf Anpassungen zu verlangen, um die Einhaltung der DSGVO sicherzustellen.

**6. Regelmäßige Überprüfung, Bewertung und Evaluierung**

Es ist ein umfassendes Informationssicherheits- (ISMS) und Datenschutzmanagementsystem (DSMS) implementiert.

The restoration of backups is regularly tested.

The IT systems have an uninterruptible power supply.

The server room has a fire alarm system and a

CO2 extinguishing system.

All server systems are subject to monitoring that triggers alerts to an administrator in the event of disturbances. An emergency plan, which also includes a restart plan, is in place.

**4. Order Control**

When external service providers or third parties are involved, a data processing agreement is concluded in accordance with the requirements of the applicable data protection law. Contractors are audited initially and then regularly.

**5. Privacy by Design and Privacy by Default**

The processor commits to ensuring data protection through technical and organizational measures (Privacy by Design) and implementing privacy-friendly defaults (Privacy by Default).

These measures aim to ensure personal data is kept to a minimum and processed only according to the controller's instructions. The processor is responsible for adhering to these principles throughout the entire development and operational processes. The controller reserves the right to regularly inspect the measures and make adjustments as needed to ensure GDPR compliance.

**6. Regular Review, Assessment and Evaluation**

A comprehensive information security management system (ISMS) and data protection management system (DPMS) is implemented.

There is a guideline on information security and data protection and policies to ensure that the objectives of the guideline are implemented. The guideline and the policies are regularly evaluated with regard to their effectiveness and adapted.

An experienced data privacy officer has been appointed and an information security and data protection team (ISDPT) has been set up to plan, implement, evaluate and make adjustments to all measures in the area of information security and data protection.

It is ensured that information security and data protection incidents are identified by all employees and reported immediately to the ISDPT. The ISDPT will investigate the incident immediately. If data processed on behalf of customers is affected, care is taken to ensure that they are informed immediately about the nature and scope of the incident.



Es gibt eine Leitlinie zu Informationssicherheit und Datenschutz und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird. Die Leitlinie und die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist ein fachkundiger betrieblicher Datenschutzbeauftragter benannt und es ist ein Informationssicherheits- und Datenschutzteam (ISDST) eingerichtet, das sämtliche Maßnahmen im Bereich von Informationssicherheit und Datenschutz plant, umsetzt, evaluiert und Anpassungen vornimmt.

Es ist sichergestellt, dass Informationssicherheits und Datenschutz-vorfälle von allen Mitarbeitern erkannt und unverzüglich dem ISDST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

## ANHANG IV:
## LISTE DER UNTERAUFTRAGSVERARBEITER

## ANNEX IV:
## LIST OF SUB-PROCESSORS

| **Unterauftragsverarbeiter (Name und Adresse)**<br>**Sub-Processor (Name and Address)** |
| --- |
| Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg |
| **Verarbeitungstätigkeit(en)**<br>**Processing Operation(s)** |
| Cloud-Computing |
| **Ort(e) der Datenverarbeitung und ggf. geeignete Garantien**<br>**Location(s) of Data Processing and, if applicable, appropriate safeguards** |
| Frankfurt am Main, Germany<br>https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf |

| **Unterauftragsverarbeiter (Name und Adresse)**<br>**Sub-Processor (Name and Address)** |
| --- |
| Klaviyo, 125 Summer Street, Floor 6, Boston, MA 02110, United States |
| **Verarbeitungstätigkeit(en)**<br>**Processing Operation(s)** |
| E-Mail Marketing |
| **Ort(e) der Datenverarbeitung und ggf. geeignete Garantien**<br>**Location(s) of Data Processing and, if applicable, appropriate safeguards** |
| United States of America<br>https://www.klaviyo.com/legal/data-processing-agreement |

| **Unterauftragsverarbeiter (Name und Adresse)**<br>**Sub-Processor (Name and Address)** |
| --- |
| Hotjar Ltd, Dragonara Business Centre, 5. Stock, Dragonara Road,Paceville St Julian's STJ 3141, Malta |

| |
|---|
| **Verarbeitungstätigkeit(en)**<br>**Processing Operation(s)** |
| Nutzererfahrung |
| **Ort(e) der Datenverarbeitung und ggf. geeignete Garantien**<br>**Location(s) of Data Processing and, if applicable, appropriate safeguards** |
| Ireland, EU |

| |
|---|
| **Unterauftragsverarbeiter (Name und Adresse)**<br>**Sub-Processor (Name and Address)** |
| Tracify GmbH, Agnes-Pockels-Bogen 1, 80992 München |
| **Verarbeitungstätigkeit(en)**<br>**Processing Operation(s)** |
| Webanalyse |
| **Ort(e) der Datenverarbeitung und ggf. geeignete Garantien**<br>**Location(s) of Data Processing and, if applicable, appropriate safeguards** |

Frankfurt, Germany

| |
|---|
| **Unterauftragsverarbeiter (Name und Adresse)**<br>**Sub-Processor (Name and Address)** |
| Adtribute Software GmbH, Im Hart 32, DE- 82110 Germering |
| **Verarbeitungstätigkeit(en)**<br>**Processing Operation(s)** |
| Cloud-basierte Marketing- und Analytikdienste |
| **Ort(e) der Datenverarbeitung und ggf. geeignete Garantien**<br>**Location(s) of Data Processing and, if applicable, appropriate safeguards** |
| Europäische Union |