Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 abs. 7 DSGVO

Durchführungsbeschluss (EU) 2021/915 der Europäischen Kommission vom 04.06.2021, veröffentlicht am 07.06.2021

Data processing agreement (DPA)

according to Art. 28 para. 7 GDPR

Implementing Decision (EU) 2021/915 of the European Commission of 4 June 2021, published on 7 June 2021

Version July 2025

zwischen

between

Company:

Street:

Postal Code, City:

Country:

im Folgenden "Verantwortliche(r) oder Auftraggeber" -

- In the following referred to as the "controller(s) or client" -

und

and

Bee360 GmbH
Victor-Gollancz-Strasse 3
76131 Karlsruhe
Germany

- im Folgenden: „Auftragsverarbeiter oder Auftragnehmer“–

- hereinafter: "Processor(s) or Contractor" -

ABSCHNITT I

Klausel 1 - Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung des Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)] sichergestellt werden.

b) Die in **Anhang I** aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß **Anhang II**.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

SECTION I

Clause 1 - Purpose and scope of application

a) These standard contractual clauses (hereinafter referred to as "clauses") are intended to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)].

b) The controllers and processors listed in **Annex I** have agreed to these clauses to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

c) These clauses apply to the processing of personal data in accordance with **Annex II**.

d) Annexes I to IV are an integral part of the clauses.

e) These clauses apply without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These clauses do not in themselves ensure that the obligations relating to international data transfers under Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 are fulfilled.

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.

Clause 2 - Unalterability of the clauses

a) The parties undertake not to amend the clauses except to supplement or update the information provided in the annexes.

b) This does not prevent the parties from incorporating the standard contractual clauses set out in these clauses into a broader contract and adding further clauses or additional safeguards, provided that these do not directly or indirectly contradict the clauses or restrict the fundamental rights or freedoms of the data subjects.

Klausel 3 - Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Clause 3 - Interpretation

a) If the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in these clauses, these terms shall have the same meaning as in the relevant Regulation.

b) These clauses must be interpreted considering the provisions of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

c) These clauses may not be interpreted in a way that is contrary to the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or that restricts the fundamental rights or freedoms of the data subjects.

Klausel 4 - Vorrang

a) 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.

Clause 4 - Priority

a) In the event of any conflict between these clauses and the provisions of any related agreements existing or subsequently entered into or concluded between the parties, these clauses shall prevail.

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 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.

Clause 5 - Tying clause

a) An entity that is not a party to these Clauses may, with the consent of all parties, accede to these Clauses as a Controller or Processor at any time by completing the Annexes and signing **Annex I**.

b) After completing and signing the annexes referred to in point (a), the acceding organization shall be treated as a party to these clauses and shall have the rights and obligations of a controller or processor in accordance with its designation in **Annex I**.

c) No rights or obligations arising from these clauses shall apply to the acceding organization for the period prior to its accession as a party.

ABSCHNITT II - PFLICHTEN DER PARTEIEN

SECTION II - OBLIGATIONS OF THE PARTIES

Klausel 6 - Beschreibung der Verarbeitung

a) 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.

Clause 6 - Description of the processing

a) The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the controller, are set out in **Annex II**.

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 Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

Clause 7 - Obligations of the parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless it is obliged to do so under Union law or the law of a Member State to which it is subject. In such a case, the processor shall inform the controller of these legal requirements prior to processing, unless the law in question prohibits this due to an important public interest. The controller may issue further instructions for the entire duration of the processing of personal data. These instructions must always be documented.

b) The processor shall inform the controller immediately if it believes that instructions issued by the controller violate Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or applicable Union or Member State data protection provisions.

7.2. Zweckbindung

a) 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.

7.2 Earmarking

a) The processor shall process the personal data only for the specific purpose(s) set out in **Annex II**, unless it receives further instructions from the controller.

7.3. Dauer der Verarbeitung personenbezogener Daten

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

7.3 Duration of the processing of personal data

a) The data shall only be processed by the processor for the duration specified in **Annex II**.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in **Anhang III** aufgeführten technischen und organisatorischen Maßnahmen in Einklang mit Art. 32 DSGVO, 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.

7.4 Security of processing

a) The Processor shall take at least the technical and organizational measures listed in **Annex III** in accordance with Art. 32 GDPR to ensure the security of the Personal Data. This shall include the protection of the data against a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, the data, whether accidental or unlawful (hereinafter "Personal Data Breach"). In assessing the appropriate level of protection, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, circumstances and purposes of the processing and the risks involved for the data subjects.

b) The Processor shall grant its personnel access to the personal data subject to processing only to the extent strictly necessary for the performance, management and monitoring of the Contract. The Processor shall ensure that the persons authorized to process the personal data received have undertaken to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality.

7.5. Sensible Daten

a) 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.

7.5 Sensitive data

a) If the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation of a person, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards.

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 von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

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 Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 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.

7.6 Documentation and compliance with the clauses

a) The parties must be able to prove compliance with these clauses.

b) The Processor shall process requests from the Controller regarding the processing of data in accordance with these Clauses promptly and appropriately.

c) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in these Clauses and arising directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the request of the Controller, the Processor shall also authorise and contribute to an audit of the processing activities covered by these Clauses at appropriate intervals or where there are indications of non-compliance. When deciding on an inspection or audit, the controller may take into account relevant certifications of the processor.

d) The controller may carry out the audit itself or commission an independent auditor. The audits may also include inspections of the processor's premises or physical facilities and shall be carried out with reasonable prior notice where appropriate.

e) The Parties shall make the information referred to in this clause, including the results of audits, available to the competent supervisory authority(ies) upon request.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen

7.7 Use of subcontracted processors

a) The Processor shall not subcontract any of its processing operations that it carries out on behalf of the Controller pursuant to these Clauses to a subprocessor without the prior separate written authorization of the Controller. The Processor shall submit the request for the separate authorization prior to engaging the relevant sub-processor, together with the information necessary for the Controller to decide on the authorization. The list of

mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in **Anhang IV**. Die Parteien halten **Anhang IV** jeweils auf dem neuesten Stand.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, 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 Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 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.

sub-processors authorized by the Controller can be found in **Annex IV**. The Parties shall keep **Annex IV** up to date.

b) Where the Processor engages a sub-processor to carry out certain processing activities (on behalf of the Controller), such engagement shall be by way of a contract which imposes on the sub-processor substantially the same data protection obligations as those applicable to the Processor under these Clauses. The Processor shall ensure that the Sub-Processor fulfils the obligations to which the Processor is subject under these Clauses and under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The Processor shall provide the Controller with a copy of any such subcontracting agreement and any subsequent amendments at the Controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may obscure the wording of the agreement before providing a copy.

d) The Processor shall be fully liable to the Controller for ensuring that the Sub-Processor fulfils its obligations under the contract concluded with the Processor. The Processor shall notify the Controller if the Sub-Processor fails to fulfil its contractual obligations.

e) The processor agrees a third-party beneficiary clause with the sub-processor, according to which the controller - in the event that the processor no longer exists in fact or in law or is insolvent - has the right to terminate the subcontracting agreement and instruct the sub-processor to delete or return the personal data.

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 stehen.

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 Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

7.8 International data transfers

a) Any transfer of data by the processor to a third country or an international organization shall take place exclusively on the basis of documented instructions from the controller or to comply with a specific provision under Union law or the law of a Member State to which the processor is subject and must comply with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The Controller agrees that in cases where the Processor utilizes a sub-processor pursuant to clause 7.7 for the performance of certain processing activities (on behalf of the controller) and these 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 may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for the application of these standard contractual clauses are met.

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

Clause 8 - Support of the person responsible

a) The processor shall inform the controller immediately of any request received from the data subject. It shall not respond to the request itself unless it has been authorized to do so by the controller.

b) Taking into account the nature of the processing, the processor shall assist the controller in the fulfilment of the controller's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations under points (a) and (b), the processor shall follow the instructions of the controller.

c) In addition to the Processor's obligation to assist the Controller pursuant to Clause 8(b), the Processor shall also assist the Controller in complying with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

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;

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 Artikel 32 der Verordnung (EU) 2016/679]

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.

1) Obligation to carry out an assessment of the impact of the intended processing operations on the protection of personal data (hereinafter "data protection impact assessment") if a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2) Obligation to consult the competent supervisory authority(ies) prior to processing if a data protection impact assessment indicates that the processing would result in a high risk, unless the controller takes measures to mitigate the risk;

3) Obligation to ensure that the personal data is accurate and up to date by the processor informing the controller without undue delay if it becomes aware that the personal data it is processing is inaccurate or out of date;

4) Obligations under Article 32 of Regulation (EU) 2016/679]

d) The Parties shall specify in **Annex III** the appropriate technical and organizational measures for the Processor to assist the Controller in the application of this Clause and the scope and extent of the assistance required.

Klausel 9 - Meldung von Verletzungen des Schutzes personenbezogener Daten

a) 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 Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der

Clause 9 - Notification of personal data breaches

a) In the event of a personal data breach, the Processor shall cooperate with and assist the Controller to enable the Controller to fulfil its obligations pursuant to Articles 33 and 34 of Regulation (EU) 2016/679 or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725, taking into account the nature of the processing and the information available to the Processor.

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);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] oder 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.

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;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679] oder [die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn

9.1 Violation of the protection of data processed by the controller

In the event of a personal data breach in connection with the data processed by the controller, the processor shall assist the controller as follows:

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

b) when obtaining the following information to be provided in accordance with Article 33(3) of Regulation (EU) 2016/679] or in the controller's notification, which shall include at least the following information:

   1) the nature of the personal data, where possible, indicating the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   2) the likely consequences of a personal data breach;

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

If and to the extent that not all such information can be provided at the same time, the initial notification will contain the information available at that time and further information will be provided as soon as it becomes available without undue delay thereafter;

c) in complying with the obligation under Article 34 of Regulation (EU) 2016/679] or [to notify the data subject without undue delay of a personal data breach where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

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);

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 Artikel 33 und 34 der Verordnung (EU) 2016/679] oder zu unterstützen.

9.2 Violation of the protection of data processed by the processor

In the event of a personal data breach in connection with the data processed by the processor, the processor shall notify the controller immediately after becoming aware of the breach. This notification must contain at least the following information:

a) a description of the nature of the breach (if possible, specifying the categories and approximate number of data subjects affected and the approximate number of data records affected);

b) Contact details of a contact point where further information about the personal data breach can be obtained;

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

If and to the extent that not all such information can be provided at the same time, the initial notification will contain the information available at that time and further information will be provided as soon as it becomes available without undue delay thereafter.

The Parties shall specify in **Annex III** any other information that the Processor must provide in order to fulfil or assist the Controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

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 Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

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

SECTION III - FINAL PROVISIONS

Clause 10 - Breaches of the clauses and termination of the contract

a) Without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, if the Processor fails to fulfil its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until it complies with these Clauses or the contract is terminated. The processor shall inform the controller immediately if, for whatever reason, it is unable to comply with these clauses.

b) The controller is authorized to terminate the contract insofar as it relates to the processing of personal data in accordance with these clauses if

   1) the controller has suspended the processing of personal data by the processor in accordance with point (a) and compliance with these clauses has not been restored within a reasonable period and in any event within one month of the suspension;

   2) the processor materially or persistently breaches these clauses or fails to fulfil its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

   3) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority(ies) relating to its obligations under these Clauses, Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The Processor shall be entitled to terminate the Contract insofar as it relates to the processing of Personal Data under these Clauses if the Controller insists on the fulfilment of its instructions after being informed by the Processor that its instructions violate applicable legal requirements under Clause 7.1(b).

d) Upon termination of the contract, the processor shall, at the choice of the controller, erase all personal data processed on behalf of the controller and certify to the controller that this has been done, or return all personal data to the controller and erase existing copies, unless there is an obligation to retain the personal data under Union or Member State law. Until

rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

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.

the deletion or return of the data, the processor shall continue to ensure compliance with these clauses.

ANHANG I
Liste der Parteien

ANNEX I
List of parties

Responsible persons:

Name:

Address:

Contact:

Name:

Position:

Place, Date:

_____

Name:

Position:

Place, Date:

_____

Data Processor:

Name: **Bee360 GmbH**

Address: **Victor-Gollancz-Strasse 3, 76137 Karlsruhe, Germany**

Contact: **security_and_compliance@bee360.com**

Philipp Hansert

Chief Revenue Officer

Karlsruhe,

_____

Alexander Schuster

Chief Technology Officer

Karlsruhe,

_____

ANHANG II

Beschreibung der Verarbeitung

Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung besteht in der Durchführung der im Hauptvertrag vereinbarten Tätigkeiten, insbesondere der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen zu den unten genannten Zwecken.

Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen gemäß Art. 28 Abs. 3 lit. a DSGVO und umfasst sämtliche im Rahmen der Dienstleistung erforderlichen Verarbeitungsschritte.

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Beschäftigte
- Kunden
- Lieferanten

Kategorien personenbezogener Daten, die verarbeitet werden

- Personenbezogene Stammdaten
- Projektrollen
- Mitarbeiterkapazitäten
- Nutzungsdaten

Art der Verarbeitung

- Offenlegung durch Übermittlung

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

- Darstellung und Verwaltung interner Prozesse
- Wartung & Pflege von IT-Systemen
- Entwicklung/Optimierung
- Hosting

Dauer der Verarbeitung

- Vertragsdauer

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

ANNEX II

Description of the processing

Purpose of the processing

The purpose of the processing is to carry out the activities agreed in the main contract, in particular the processing of personal data on behalf of the controller for the purposes specified below.

The processing is carried out exclusively on the documented instructions of the controller in accordance with Art. 28 para. 3 lit. a GDPR and includes all processing steps required as part of the service.

Categories of data subjects whose personal data are processed

- Employees
- Customers
- Suppliers

Categories of personal data that are processed

- Personal master data
- Project roles
- Employee capacities
- Usage data

Type of processing

- Disclosure by transmission

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

- Visualization and management of internal processes
- Maintenance & care of IT systems
- Development/Optimization
- Hosting

Duration of processing

- Contract duration

In the case of processing by (sub)processors, the object, type and duration of the processing must also be stated.

- NTT Data Deutschland GmbH als Unterstützer in Optimierung, Entwicklung, Wartung und Support, Hosting durch Offenlegung durch Übermittlung	- NTT Data Deutschland GmbH as a supporter in optimization, development, maintenance and support, hosting through disclosure by transmission

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

ANNEX III

Technical and organizational measures, including to ensure the security of data

ALLGEMEINES

GENERAL

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen geschieht im Rahmen des Informationssicherheitsmanagements basierend auf dem etablierten ISMS (siehe auch Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit).

Procedures for regularly reviewing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing

The regular review, assessment and evaluation of the effectiveness of the technical and organizational measures is carried out as part of information security management based on the established ISMS (see also Measures for internal governance and management of IT and IT security).

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Die im Rahmen des ISMS bestehende Richtlinie zur Kommunikationssicherheit beschreibt die Netzwerktopologie und Netzwerkseparierung sowie die installierte Sicherheitssoftware und weitere Sicherheitsmaßnahmen, wie zum Beispiel Verschlüsselung, in Bezug auf die Ausgestaltung und Konfiguration der separierten Netzwerke. Die Standardkonfiguration von Systemzugängen leitet sich aus den in der Richtlinie zur Zugangskontrolle definierten Anwenderprofilen sowie aus der Richtlinie für sichere Passwörter ab. Darüber hinaus existieren weitere Standardkonfigurationen für alle Systeme und Anwendungen unter Berücksichtigung der Anforderungen an die Informationssicherheit sowie die DSGVO. Die Einhaltung der Konfigurationsstandards wird durch den Einsatz automatisierter Konfigurationsmanagement-Tools unterstützt und regelmäßig überprüft. Eine regelmäßige Wartung der Systeme stellt die Versorgung mit aktuellen Sicherheitsupdates und Patches sicher. Die verantwortlichen Mitarbeiter werden regelmäßig bezüglich der Bedeutung einer sicheren Systemkonfiguration sensibilisiert.

Measures to ensure the system configuration, including the default configuration

The existing policy on communication security as part of the ISMS describes the network topology and network separation as well as the installed security software and other security measures, such as encryption, in relation to the design and configuration of the separated networks. The standard configuration of system access is derived from the user profiles defined in the access control policy and the policy for secure passwords. In addition, there are further standard configurations for all systems and applications, taking into account information security requirements and the GDPR. Compliance with the configuration standards is supported and regularly checked by the use of automated configuration management tools. Regular maintenance of the systems ensures the supply of current security updates and patches. The responsible employees are regularly sensitized to the importance of secure system configuration.

-

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Die interne Governance und Verwaltung der IT und der IT-Sicherheit basiert auf einem etablierten Informationssicherheitsmanagementsystems (ISMS) entlang des TISAX/ISO27001-Rahmenwerks. Dies beinhaltet die Durchführung von Risikoanalysen und die Verwaltung von Schwachstellen, ebenso wie die Implementierung von Sicherheitsrichtlinien zur Kontrolle des Zugriffs auf IT-Systeme und Daten, die Sicherstellung der Integrität und Vertraulichkeit von Informationen sowie die Einhaltung der Datenschutzgesetze.

Measures for the internal governance and management of IT and IT security

The internal governance and management of IT and IT security is based on an established information security management system (ISMS) in line with the TISAX/ISO27001 framework. This includes conducting risk analyses and managing vulnerabilities, as well as implementing security policies to control access to IT systems and data, ensuring the integrity and confidentiality of information and complying with data protection laws.

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Das bestehende TISAX Label (Standard Scope 2.0) ist auf ENX veröffentlicht. Darüber hinaus ist ein externer Datenschutzbeauftragter bestellt, der ebenfalls entsprechend zertifiziert ist (TÜV, CIPP/E).

Measures for the certification/quality assurance of processes and products

The existing TISAX label (Standard Scope 2.0) published on ENX. In addition, an external data protection officer has been appointed who is also certified accordingly (TÜV, CIPP/E).

Maßnahmen zur Gewährleistung der Datenminimierung und zur Vermeidung einer Vorratsdatenspeicherung

Die Datenminimierung wird unter Konsultation des externen Datenschutzbeauftragen in Form eines individuellen Löschkonzepts für die unterschiedlichen Informationswerte (Assets) gewährleistet. Das Löschkonzept wird bezogen auf die als Auftragsverarbeiter geleisteten Datenverarbeitungsprozesse unter Berücksichtigung der Zweckbindung sowie der Rechtmäßigkeit umgesetzt. Bestehende nationale Aufbewahrungsfristen werden gewahrt.

-

Measures to ensure data minimization and to avoid data retention

Data minimization is ensured in consultation with the external data protection officer in the form of an individual erasure concept for the various information assets. The deletion concept is implemented in relation to the data processing processes carried out as a processor, taking into account the purpose limitation and legality. Existing national retention periods are observed.

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Die Zusammenarbeit mit dem externen Datenschutzbeauftragten erfolgt über digitale Plattformen, in denen alle wesentlichen Dokumente in schriftlicher Fassung abgelegt werden. Dies umfasst unter anderem die Dokumentation von Datenverarbeitungsaktivitäten, die Implementierung von Datenschutzrichtlinien, die Schulung und Sensibilisierung der Mitarbeiter (Zertifikate) sowie rechtliche Anfragen und Verläufe.

Measures to ensure accountability

Collaboration with the external data protection officer takes place via digital platforms in which all key documents are stored in written form. This includes the documentation of data processing activities, the implementation of data protection guidelines, the training and sensitization of employees (certificates) as well as legal enquiries and processes.

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Die Übertragbarkeit personenbezogener Daten wird durch die Verwendung standardisierter Datenformate ermöglicht. Betroffene Personen haben die Möglichkeit ihre personenbezogenen Daten in einem maschinenlesbaren Format zu erhalten. Die Umsetzung der Löschkonzepte wird durch automatisierte Löschverfahren unterstützt. Personenbezogene Daten werden gemäß den gesetzlichen Anforderungen gelöscht.

Measures to enable data portability and to ensure erasure

The portability of personal data is made possible through the use of standardized data formats. Data subjects have the option of receiving their personal data in a machine-readable format. The implementation of the erasure concepts is supported by automated erasure procedures. Personal data is erased in accordance with legal requirements.

VERTRAULICHKEIT

CONFIDENTIALITY

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Die im Rahmen des ISMS bestehende Richtline zur Systembeschaffung und -entwicklung regelt die Pseudonymisierung personenbezogener Daten. Im Falle einer Pseudonymisierung werden persönliche, direkte Identifikatoren durch zufällig generierte Pseudonyme ersetzt. Die ursprünglichen Identifikatoren sind in von den Pseudonymen getrennten Datensätzen gespeichert. Ein rollenbasiertes Berechtigungskonzept mit streng getrennten Nutzerprofilen, stellt sicher, dass nur autorisierten Personen eine Verknüpfung von Pseudonymen und Identifikatoren möglich ist.

Die im Rahmen des ISMS bestehende Richtlinie zur Verschlüsselung legt die Verwendung starker Verschlüsselungsalgorithmen nach aktuellen Standards fest und regelt die sichere Schlüsselverwaltung. Basierend auf den durch die Richtlinie erlaubten Algorithmen und Protokollen ist die Datenübertragung über Netzwerke grundsätzlich TLS-verschlüsselt. Remote Zugriffe erfolgen über VPN bzw. SSH. Festplattenverschlüsselung ist über FileVault bzw. Bitlocker gewährleistet.

Measures for pseudonymization and encryption of personal data

The existing guideline for system procurement and development as part of the ISMS regulates the pseudonymization of personal data. In the case of pseudonymization, personal, direct identifiers are replaced by randomly generated pseudonyms. The original identifiers are stored in data records that are separate from the pseudonyms. A role-based authorization concept with strictly separate user profiles ensures that only authorized persons are able to link pseudonyms and identifiers.

The existing policy on encryption as part of the ISMS specifies the use of strong encryption algorithms in accordance with current standards and regulates secure key management. Based on the algorithms and protocols permitted by the policy, data transmission via networks is always TLS-encrypted. Remote access takes place via VPN or SSH. Hard drive encryption is guaranteed via FileVault or Bitlocker.

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Die im Rahmen des ISMS bestehende Richtlinie zu Zugängen und Zugangsmöglichkeiten verbietet die Erstellung kollektiver Benutzerkonten sowie die gemeinsame Nutzung von Konten. Entsprechend werden ausschließlich individuelle Benutzerkonten verwendet, die eine eindeutige Identifikation gewährleisten. Starke Authentifizierungsmethoden wie MFA und sichere Passwörter entsprechend einer organisationsweiten

Measures to identify and authorize users

The existing policy on access and access options as part of the ISMS prohibits the creation of collective user accounts and the sharing of accounts. Accordingly, only individual user accounts that guarantee unique identification are used. Strong authentication methods such as MFA and secure passwords in accordance with an organization-wide password policy further increase the security of identification. Single sign-on simplifies login from the user's perspective and increases the acceptance of secure

Passwortrichtlinie erhöhen die Sicherheit der Identifikation zusätzlich. Single-Sign-On erleichtert die Anmeldung aus Anwendersicht und steigert die Akzeptanz sicherer Passwörter. Während des Registrierungsprozesses und bei Passwortänderungen wird die Identität des Benutzers automatisiert oder manuell verifiziert.

Die im Rahmen des ISMS bestehende Zugriffsrichtlinie definiert Benutzerprofile nach dem Prinzip des geringsten Privilegs. Diese Benutzerprofile sowie das in der Applikation Bee360 verankerte Rollen- und Berechtigungskonzept bilden die Grundlage der rollenbasierten Zugriffskontrolle (RBAC). Die Autorisierung der Nutzer wird protokolliert und zeitlich auf die erforderliche Zeitspanne begrenzt. Im Rahmen des Berechtigungsmanagements, werden Zuweisung, Änderung und Aufhebung von Zugriffsrechten entlang definierter Prozesse verwaltet. Die etablierten Notfallzugriffsverfahren stellen außerdem sicher, dass nur autorisierte Personen im Notfall die nötigen erweiterten Zugriffsrechte erhalten.

passwords. The user's identity is verified automatically or manually during the registration process and when passwords are changed.

The existing access policy as part of the ISMS defines user profiles according to the principle of least privilege. These user profiles and the role and authorization concept anchored in the Bee360 application form the basis of role-based access control (RBAC). User authorization is logged and limited to the required period of time. As part of authorization management, the assignment, modification and cancellation of access rights are managed according to defined processes. The established emergency access procedures also ensure that only authorized persons receive the necessary extended access rights in an emergency.

Maßnahmen zum Schutz der Daten während der Übermittlung

Die im Rahmen des ISMS bestehende Richtlinie zur Verschlüsselung legt die Verwendung starker Verschlüsselungsalgorithmen nach aktuellen Standards fest und regelt die sichere Schlüssel- und Zertifikatsverwaltung. Basierend auf den durch die Richtlinie erlaubten Algorithmen und Protokollen ist die Datenübertragung über Netzwerke grundsätzlich TLS-verschlüsselt. Remote Zugriffe erfolgen über VPN bzw. SSH (siehe auch Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten). Die Kommunikationssicherheitsrichtlinie regelt für alle Mitarbeiter, über welche Kommunikationskanäle Informationen übermittelt werden dürfen. Die Verhaltensregeln für die Übermittlung von Information hängen zum einen vom genutzten Kommunikationskanal, zum anderen von der Klassifizierung der Information in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit ab und sind durch die Kommunikationssicherheitsrichtlinie und die Richtlinie zur Informationsklassifizierung festgelegt.

Measures to protect data during transmission

The existing policy on encryption as part of the ISMS specifies the use of strong encryption algorithms in accordance with current standards and regulates secure key and certificate management. Based on the algorithms and protocols permitted by the policy, data transmission via networks is always TLS-encrypted. Remote access takes place via VPN or SSH (see also measures for pseudonymization and encryption of personal data). The communication security policy regulates for all employees which communication channels may be used to transmit information. The rules of behavior for the transmission of information depend on the communication channel used and on the classification of the information in terms of confidentiality, integrity and availability and are defined by the communication security policy and the information classification policy.

Maßnahmen zum Schutz der Daten während der Speicherung

Die im Rahmen des ISMS bestehende Richtlinie zur Verschlüsselung legt die Verwendung starker Verschlüsselungsalgorithmen nach aktuellen Standards

Measures to protect data during storage

The existing policy on encryption as part of the ISMS specifies the use of strong encryption algorithms in accordance with current standards and regulates secure key management. Based on the algorithms and protocols

fest und regelt die sichere Schlüsselverwaltung. Basierend auf den durch die Richtlinie erlaubten Algorithmen und Protokollen wird die Festplattenverschlüsselung über FileVault bzw. Bitlocker gewährleistet (siehe auch Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten). Die bestehende Zugriffsrichtlinie definiert Benutzerprofile nach dem Prinzip des geringsten Privilegs (siehe auch Maßnahmen zur Identifizierung und Autorisierung der Nutzer). Diese Benutzerprofile sowie separate Administratorkonten gewährleisten, dass nur autorisierte Personen auf gespeicherte Daten zugreifen können. Ereignisse wie erfolgreiche und fehlgeschlagene Anmeldeversuche oder die Änderung von Benutzerrechten werden gemäß der bestehenden Protokollierungsrichtlinie erfasst (siehe auch Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen). Die Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden, werden im nächsten Abschnitt beschrieben und tragen, neben physisch getrennten Sicherungskopien, ebenfalls zum Schutz der Daten während der Speicherung bei. Darüber hinaus bestehen Maßnahmen und Verhaltensregeln, die sich an der Klassifizierung der Daten gemäß der bestehenden Richtlinie zur Informationsklassifizierung orientieren. Beispiele hierfür sind der zusätzliche Passwortschutz einzelner Dokumente, die Speicherung nur auf internen Servern oder die sofortige Löschung von lokalen Kopien nach der Nutzung. Zum Schutz vor Malware kommen Betriebssystem-Firewalls sowie Abwehrsysteme wie Windows Defender oder Apple Gatekeeper zum Einsatz. Zusätzlich finden regelmäßige Schulungen der Mitarbeiter statt um diese für die Gefahren, zum Beispiel durch Phishing-Praktiken, zu sensibilisieren. Die bestehende Richtlinie zur akzeptierten Nutzung von Informationswerten regelt außerdem den grundsätzlichen Umgang mit Client-Rechnern und Serversystemen. Dies umfasst insbesondere das Installations- und Nutzungsverbot bestimmter Software. Gespeicherte Daten, die nicht mehr benötigt werden, werden gemäß der bestehenden Richtlinie zu Entsorgung und Vernichtung sicher gelöscht.

permitted by the policy, hard disk encryption is ensured via FileVault or Bitlocker (see also measures for pseudonymization and encryption of personal data). The existing access policy defines user profiles according to the principle of least privilege (see also Measures for identifying and authorizing users). These user profiles and separate administrator accounts ensure that only authorized persons can access stored data. Events such as successful and failed login attempts or changes to user rights are recorded in accordance with the existing logging policy (see also Measures to ensure the logging of events). The measures to ensure the physical security of locations where personal data is processed are described in the next section and, in addition to physically separate backup copies, also contribute to the protection of data during storage. In addition, there are measures and rules of behavior that are based on the classification of data in accordance with the existing information classification policy. Examples of this are the additional password protection of individual documents, storage only on internal servers or the immediate deletion of local copies after use. Operating system firewalls and defense systems such as Windows Defender or Apple Gatekeeper are used to protect against malware. In addition, regular training courses are held for employees to sensitize them to the dangers of phishing practices, for example. The existing policy on the acceptable use of information assets also regulates the basic handling of client computers and server systems. In particular, this includes a ban on the installation and use of certain software. Stored data that is no longer required is securely deleted in accordance with the existing policy on disposal and destruction.

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Zu den Bürostandorten haben die Mitarbeiter über Schlüsselkarten oder physische Schlüssel Zugang. Die Ausgabe und Rückgabe derselben wird in einer Schlüsselliste dokumentiert und quittiert. Besucher dürfen die Bürostandorte nur in Begleitung eines Mitarbeiters

Measures to ensure the physical security of places where personal data processed

Employees have access to the office locations via key cards or physical keys. The issue and return of these is documented and receipted in a key list. Visitors may only enter the office locations when accompanied by an employee. Security personnel monitor the premises, particularly at night.

betreten. Sicherheitspersonal überwacht die Räumlichkeiten insbesondere nachts.

Gemäß der Richtlinie zum sauberen Schreibtisch und klaren Bildschirm und der Richtlinie zum mobilen Arbeiten schützt jeder Mitarbeiter seinen Arbeitsplatz durch zum Beispiel Sperrung des Bildschirms und Entfernen von Papierdokumenten und Datenträgern bei Abwesenheit bzw. durch Sichtschutzfolien und Laptop-Schlösser. Dies ist insbesondere durch regelmäßige Schulungen und die Sensibilisierung der Mitarbeiter für die Notwendigkeit erhöhter Wachsamkeit im Homeoffice und im öffentlichen Raum gewährleistet. Darüber hinaus regelt die Richtline zum sauberen Schreibtisch und klaren Bildschirm den Zugang und die Nutzung des zentralen Mutifunktionsdruckers in den gemeinschaftlich genutzten Büroräumen.

Das Rechenzentrum wird von einem Dienstleister betrieben und ist zertifiziert gemäß ISO 27001. Dies umfasst folgende Maßnahmen zum Schutz gegen unbefugten Zugang:

- Detaillierte Verwaltung der Zutrittsberechtigungen
- Organisatorische Anweisungen zur Meldung von Austritten, Beurlaubungen etc. an das Zutrittsverwaltungssystem
- Spezielle Schließverfahren, elektronische Zugangskontrolle
- Zugangskontrolle am Empfang
- Videoüberwachung
- Sicherheitspersonal
- Keine Fenster/Fensterlosigkeit
- Einbruchsichere Türen
- Bewegungsdetektoren

Zugang wird ausschließlich bestimmten Bee360 Mitarbeitern gewährt, die als zugangsberechtigt beim Dienstleister registriert sind. Der Zugang von Bee360 Mitarbeitern findet immer in Begleitung eines Mitarbeiters des Dienstleisters statt. Jeder Zugang ins Rechenzentrum wird vom Dienstleister protokolliert.

Das Rechenzentrum und die darin befindlichen Datenträger sind wie folgt gegen Umweltbedrohungen geschützt:

- Rauch- und Feuermelder
- Brandmeldeanlagen mit direkter Aufschaltung auf die Feuerwehr

In accordance with the clean desk and clear screen policy and the mobile working policy, every employee protects their workplace by, for example, locking the screen and removing paper documents and data carriers when they are absent or by using privacy screens and laptop locks. This is ensured in particular through regular training and by sensitizing employees to the need for increased vigilance when working from home and in public spaces. In addition, the guidelines on clean desks and clear screens access to and use of the central multifunction printer in shared office spaces.

The data center is operated by a service provider and is certified in accordance with ISO 27001, which includes the following measures to protect against unauthorized access:

- Detailed management of access authorizations
- Organizational instructions for reporting departures, leaves of absence, etc. to the access management system
- Special locking procedures, electronic access control
- Access control at reception
- Video surveillance
- Security personal
- No windows/windowless
- Burglar-proof doors
- Motion detectors

Access is only granted to certain Bee360 employees who are registered with the service provider as authorized users. Access by Bee360 employees is always accompanied by an employee of the service provider. All access to the data center is logged by the service provider.

The data center and the data carriers in it are protected against environmental threats as follows:

- Smoke and fire alarms
- Fire alarm systems with direct connection to the fire brigade
- Fire doors
- Water protection facilities
- Shielding attenuation
- Emergency power supply
- Standardized procedure for regularly reviewing the appropriateness of the protective measures taken

- Feuerschutztüren
- Wasserschutzeinrichtungen
- Schirmdämpfung
- Notstromversorgung
- Standardisiertes Verfahren zur regelmäßigen Überprüfung der Angemessenheit der getroffenen Schutzmaßnahmen
- Hausordnung, die den Zutritt nur nach Schulung/Unterweisung oder in Begleitung erlaubt

- House rules that only allow access after training/instruction or under escort

INTEGRITÄT

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Die im Rahmen des ISMS bestehende Protokollierungsrichtlinie legt die Art und Form der zu protokollierenden Ereignisse sowie entsprechende Aufbewahrungszeiten fest. Die konkreten Festlegungen hängen von der Klassifizierung des jeweiligen Systems ab und umfassen unter anderem erfolgreiche und fehlgeschlagene Anmeldeversuche, die Änderung von Benutzerrechten, sowie das Starten und Beenden von Prozessen. Die Protokolle werden in standardisierten Formaten erfasst und enthalten detaillierte, einheitliche und über die Systeme zeitlich synchronisierte Zeitstempel sowie eindeutige Benutzer-IDs und IDs der Protokollquellen. Dies ermöglicht die zentralisierte Auswertung der Protokolldaten.

Maßnahmen zur Gewährleistung der Datenqualität

Zur Sicherung der Datenqualität sind für die Applikation Bee360 auf verschiedenen Ebenen entsprechende Validierungsregeln implementiert. Korrekte Beziehungen zwischen Datenbankelementen werden, zum Beispiel, durch die Verwendung relationaler Datenbanken, die Definition von Fremdschlüsseln und durch standardisierte Datenformate gewährleistet. Automatisch importierte Daten werden mit Hilfe von eindeutigen Identifikatoren mit bestehenden Daten in Bee360 verknüpft. Verletzungen der Eindeutigkeit oder der Vollständigkeitskriterien werden automatisch abgefangen und protokolliert, so dass die zugrunde liegenden Inkonsistenten korrigiert werden können. Über Schnittstellen findet außerdem eine regelmäßige Aktualisierung relevanter Daten statt. Bei der Eingabe von Daten durch die Anwender werden ebenfalls

INTEGRITY

Measures to ensure the logging of events

The logging policy in place as part of the ISMS specifies the type and form of events to be logged and the corresponding retention periods. The specific specifications depend on the classification of the respective system and include successful and failed login attempts, changes to user rights and the starting and ending of processes. The logs are recorded in standardized formats and contain detailed, uniform time stamps that are synchronized across the systems as well as unique user IDs and log source IDs. This enables centralized evaluation of the log data.

Measures to ensure data quality

To ensure data quality, corresponding validation rules have been implemented for the Bee360 application at various levels. Correct relationships between database elements are ensured, for example, through the use of relational databases, the definition of foreign keys and standardized data formats. Automatically imported data is linked to existing data in Bee360 using unique identifiers. Violations of uniqueness or completeness criteria are automatically intercepted and logged so that the underlying inconsistencies can be corrected. Relevant data is also regularly updated via interfaces. Corresponding consistency criteria are also checked when users enter data. The user is supported by a user-friendly graphical interface when entering data. The fields of the associated forms have format and type definitions. Certain fields are

entsprechende Konsistenzkriterien überprüft. Der Anwender wird bei der Eingabe durch eine benutzerfreundliche grafische Oberfläche unterstützt. Die Felder der zugehörigen Formulare verfügen über Format- und Typdefinitionen. Bestimmte Felder sind obligatorisch oder erfordern die Eingabe eindeutiger Werte. Visuelle Hinweise informieren den Anwender, falls die eingegeben Daten, diesen Vorgaben nicht genügen. Dropdownlisten und das automatische Befüllen bestimmter Felder helfen zusätzlich die Vollständigkeit und Korrektheit der Daten sicher zu stellen. Die initiale Eingabe sowie die nachträgliche Änderung der Informationen in den Formularen wird automatisch protokolliert und in Form einer Änderungshistorie auf dem Formular angezeigt. Für die Prüfung auf inhaltliche Duplikate bietet Bee360 spezielle Berichte.

mandatory or require the entry of unique values. Visual information informs the user if the data entered does not fulfil these requirements. Drop-down lists and the automatic filling of certain fields also help to ensure that the data is complete and correct. The initial entry and subsequent changes to the information in the forms are automatically logged and displayed on the form in the form of a change history. Bee360 offers special reports to check for duplicate content.

Maßnahmen zur Gewährleistung der Datentrennung

Die Trennung der Systeme des Auftragnehmers und der Auftraggeber besteht physikalisch und/oder logisch in separaten virtuellen Umgebungen sowie durch entsprechende Netzwerksegmentierung und dedizierte Firewallregeln. Die Trennung der Applikationen von verschiedenen Auftraggebern erfolgt durch separate Datenbanken und Service-Installationen pro Applikation. Datenzugriffe sind nur entlang von definierten Rollen und Berechtigungen über separate Benutzerkonten erlaubt. Darüber hinaus besteht eine generelle Trennung von Produktiv- und Nichtproduktivsystemen in entsprechend getrennten Umgebungen. Sicherheitskopien werden für jede Kundenapplikation separat erstellt und räumlich getrennt von den aktiven Applikationen gespeichert.

Measures to ensure data separation

The contractor's and client's systems are separated physically and/or logically in separate virtual environments as well as through appropriate network segmentation and dedicated firewall rules. Separation of the applications of different clients is achieved through separate databases and service installations for each application. Data access is only permitted in accordance with defined roles and authorizations via separate user accounts. In addition, there is a general separation of productive and non-productive systems in correspondingly separate environments. Backup copies are created separately for each customer application and stored separately from the active applications.

VERFÜGBARKEIT

Maßnahmen zur Gewährleistung der jederzeitigen Verfügbarkeit

Die Bee360 Cloud nutzt eine hyperkonvergente Infrastruktur (HCI), die auf eine kontinuierliche Bereitstellung von Diensten selbst bei Ausfällen ausgelegt ist, und die eine flexible Skalierung von Ressourcen je nach Bedarf ermöglicht. Die zugrundeliegende Hardware ist redundant ausgelegt bezüglich Cluster-Knoten, Switches, Borderfirewall und Stromversorgung. Entsprechende Failover-Mechanismen ermöglichen eine Kompensation bei Hardwarestörungen.
Die Hardware ist in einem ISO-zertifizierten Rechenzentrum untergebracht und gegen Gefahren wie Überhitzung, Sabotage und Umweltbedrohungen

AVAILABILITY

Measures to ensure availability at all times

The Bee360 Cloud utilizes a hyperconverged infrastructure (HCI) that is designed for the continuous provision of services even in the event of failures and enables flexible scaling of resources as required. The underlying hardware is redundant in terms of cluster nodes, switches, border firewall and power supply. Corresponding failover mechanisms enable compensation in the event of hardware faults.
The hardware is housed in an ISO-certified data center and protected against hazards such as overheating, sabotage and environmental threats (see also Measures to ensure the physical security of locations where personal data is processed). Responsible persons have physical or

geschützt (siehe auch Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden). Verantwortliche Personen haben entsprechend ihrer Rollen und Berechtigungen im Notfall physischen bzw. administrativen Zugang.

Hardware, HCI und virtualisierte Server werden regelmäßig gewartet. Die Verfügbarkeit wird durch entsprechende Monitoringsysteme in Echtzeit überwacht. Bei Ausfällen wird automatisch alarmiert. Die anschließende Fehlerbehebung erfolgt entlang definierter Prozesse gemäß der bestehenden Richtlinie zum Verfahren für das Management von Vorfällen. Darüber hinaus bestehen Scenario basierte Handlungsanleitungen für zum Beispiel DDoS-Angriffe sowie präventive Schutzmaßnahmen gegen DDoS-Angriffe. Regelmäßige Backup-Routinen gemäß dem in der bestehenden Richtlinie zur Betriebskontinuität verankerten Datensicherungskonzept ermöglichen die Wiederherstellung der Betriebsfähigkeit bei Datenverlusten.

administrative access in an emergency in accordance with their roles and authorizations.

Hardware, HCI and virtualized servers are regularly maintained. Availability is monitored in real time using appropriate monitoring systems. Automatic alerts are sent in the event of failures. Subsequent troubleshooting is carried out in accordance with defined processes in line with the existing incident management policy. In addition, there are scenario-based instructions for action for DDoS attacks, for example, as well as preventive protective measures against DDoS attacks. Regular backup routines in accordance with the data backup concept anchored in the existing business continuity policy enable the restoration of operational capability in the event of data loss.

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Die Wiederherstellungspräferenzen für personenbezogene Daten hängen von ihrer jeweiligen Bewertung gemäß der bestehenden Richtlinie zur Informationsklassifizierung ab. Das in der Richtlinie zur Betriebskontinuität verankerte Datensicherungskonzept schreibt Wiederherstellungspläne und regelmäßige Backups vor, die die Wiederherstellung bis zu einem definierten Punkt (RPO) ermöglichen. Die Speicherung der Vollsicherungen und inkrementellen Backups in einem Datenspeicher mit Raid Level 5 stellt die Verfügbarkeit der Sicherungen sicher. Sensibilisierung der Mitarbeiter, Notfallkontaktlisten sowie streng geschützte Notfallzugänge für die entsprechenden Systeme sichern die Fähigkeit auch im Notfall schnell handeln zu können.

Measures to ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident

The recovery preferences for personal data depend on their respective assessment according to the existing information classification policy. The data backup concept anchored in the business continuity policy prescribes recovery plans and regular backups that enable recovery to a defined point (RPO). The storage of full backups and incremental backups in a data storage system with Raid Level 5 ensures the availability of the backups. Sensitization of employees, emergency contact lists and strictly protected emergency access for the relevant systems ensure the ability to act quickly in an emergency.

ANHANG IV

Liste der Unterauftragsverarbeiter

ANNEX IV

List of sub-processors

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

The controller has authorized the use of the following sub-processors:

Strategischer Partner - Unterstützer im Hosting und in der Erbringung von anderen Dienstleistungen

NTT Data Deutschland GmbH

Hans-Döllgast-Straße 26, 80807 München, Germany

Edwin Benz, Edwin.Benz@nttdata.com

Strategic partner - supporter in hosting and the provision of other services

Datacenter, in dem die Bee360-eigene Hardware für den SaaS betrieben wird

ILK Internet GmbH

Am Sandfeld 15, 76149 Karlsruhe, Germany

Kevin Chassonnaud, kch@ilk.net

Data center in which Bee360's own hardware for the SaaS is operated