Auftragsverarbeitungsvereinbarung/ Data Processing Agreement

Alasco Plattform

Stand: 07.01.2026 As of: 2026-01-07

zwischen / between

dem Kunden / the customer

nachfolgend “Verantwortlicher” / hereinafter also referred to as “controller”

und / and

Alasco GmbH

nachfolgend “Auftragsverarbeiter” / hereinafter also referred to as “processor”

nachfolgend jeweils auch “Partei” bzw. gemeinsam “Parteien” genannt / hereinafter collectively also referred to as the “party” or the “parties”.

convenient translation

	Standardvertragsklauseln	**Standard contractual clauses**
	Abschnitt I	**Section I**
	Klausel 1	**Clause 1**
1.	**Zweck und Anwendungsbereich**	**Purpose and scope**
a)	Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von 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] (“Verordnung (EU) 2016/679”) sichergestellt werden.	The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance 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)	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 zu gewährleisten.	The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) Verordnung (EU) 2016/679 and/or Article 29(3) and (4) Verordnung (EU) 2016/679.
c)	Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.	These Clauses apply to the processing of personal data as specified in Annex II.
d)	Die Anhänge I bis IV sind Bestandteil der Klauseln.	Annexes I to IV are an integral part of the Clauses.
e)	Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.	These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.
f)	Diese Klauseln stellen für sich allein genommen nicht sicher, dass die	These Clauses do not by themselves ensure compliance with obligations

Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

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.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 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 auszulegen.

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

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.

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.

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.

Klausel 5

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

Clause 5

Docking clause

Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

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.

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

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.

Section II - Obligations of the Parties

Clause 6

Description of processings

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.

Klausel 7

Pflichten der Parteien

Clause 7

Obligations of the Parties

7.1. **Weisungen**

Instructions

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.

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) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er

The processor shall immediately inform the controller if, in the processor's

der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

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. **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.

Purpose limitation

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

7.3. **Dauer der Verarbeitung personenbezogener Daten**

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

Duration of the processing of personal data

Processing by the processor shall only take place 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, 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

Security of processing

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 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.

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.

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. **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.

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 specific restrictions and/or additional safeguards.

7.6. **Dokumentation und Einhaltung der Klauseln**

Documentation of compliance

a)	Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.	The Parties shall be able to demonstrate compliance with these Clauses.
b)	Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.	The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
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 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.	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)	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.	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)	Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.	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.	**Einsatz von Unterauftragnehmern**	**Use of sub-processors**
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 30 Tage im Voraus ausdrücklich in Textform 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.	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 30 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.
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 unterliegt.	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)	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.	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)	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.	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)	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.	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.	**Internationale Datenverarbeitung**	**International transfer**
a)	Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt	Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis

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 im Einklang stehen.

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 place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

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 Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

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.

Klausel 8

Unterstützung des Verantwortlichen

Clause 8

Assistance to the controller

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

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.

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.

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) 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:

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) 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;

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) 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

2) the obligation to consult the competent supervisory 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

der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

controller to mitigate the risk;

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;

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) Verpflichtungen gemäß Artikel 32 Verordnung (EU) 2016/679.

4) the obligations in Article 32 of Regulation (EU) 2016.

8.4. 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.

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.

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 Artikeln 33 und 34 Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

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 Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

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 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

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 Article 33 (3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

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

3) the measures taken or proposed to be taken by the controller to address the

Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.	personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
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;	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.
c) bei der Einhaltung der Pflicht gemäß Artikel 34 Verordnung (EU) 2016/679 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.	in complying, pursuant to Article 34 of Regulation (EU) 2016/679, 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. **Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten**	**Data breach concerning data processed by the processor**
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:	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) eine Beschreibung der Art der Verletzung (möglichst unter	a) a description of the nature of the breach (including, where possible, the

Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

categories and approximate number of data subjects and data records concerned);

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

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

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.

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

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.

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.

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 Verordnung (EU) 2016/679 zu unterstützen.

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 Articles 33 and 34 of Regulation (EU) 2016/679.

Abschnitt III - Schlussbestimmungen

Section III - Final Provisions

Klausel 10

Clause 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 Verordnung (EU) 2016/679 – 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 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n),

Non-compliance with the clauses and termination

Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, 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.

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 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 regarding its obligations

die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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.

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.

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.

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/Annex I - Parteien & Datenschutzbeauftragte / Parties & Data Protection Officer(s)

Auftragsverarbeiter / Processor	
Name / name	**Alasco GmbH**
vertreten durch represented by	Emanuel Breitsameter, Anselm Bauer-Wohlleb, Benedict Marzahn, Moritz Gunz
Adresse / address	Leopoldstraße 21, 80802 München
Kondaktdaten / contact details:	E-mail: privacy@alasco.de Phone: +49 (0) 89 248867750
Datenschutzbeauftragter/ Data Protection Officer	DataCo GmbH Sandstraße 33, 80335 München

Verantwortlicher / Controller	
Name, Adresse und Ansprechperson ergeben sich aus dem Hauptvertrag, dem diese Auftragsverarbeitungsvereinbarung zugrunde liegt. Der Vertragspartner teilt den Namen seines Datenschutzbeauftragten bzw. seiner Ansprechperson für Datenschutzfragen gesondert mit.	Name, address and contact person can be found in the main contract on which this data processing contract is based. The customer shall provide the name of its data protection officer or its contact person for data protection issues separately.

Anhang/Annex II - Beschreibung der Verarbeitung / Description of the Data Processing

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden / Categories of data subjects whose personal data is processed	Alle Personen, die Zugriff auf die Plattform erhalten, insbesondere Mitarbeiter des Kunden, dessen Auftragnehmer, andere Stakeholder, Mieter (nur bei Nutzung der ESG-Produkte)	All persons who have access to the platform, in particular employees of the customer, their contractors, other stakeholders, tenants (ESG products only).
Kategorien personenbezogener Daten, die verarbeitet werden / Categories of personal data processed	Unternehmenszugehörigkeit, Kontaktdaten, Login-Daten, Telemetriedaten, Feedback, KI-Eingaben (soweit sie personenbezogene Daten enthalten), Energieverbrauchsdaten (nur bei Nutzung der ESG-Produkte)	Company affiliation, contact details, login details, telemetry data, feedback, AI inputs (insofar as they contain personal data), energy consumption data (ESG products only).
Verarbeitete sensible Daten/ Processed sensitive data	Es werden keine sensiblen Daten im Sinne des Art. 9 Verordnung (EU) 2016/679 verarbeitet.	No sensitive data within the meaning of Art. 9 Regulation (EU) 2016/679 is processed.
Art der Verarbeitung / Nature of the processing	**Erhebung** der Daten durch Online-Formulare, API-Schnittstellen. **Speicherung** der Daten ausschließlich verschlüsselt in einer gesicherten Cloud-Umgebung. **Nutzung** der Daten zur Bereitstellung des Dienstes, insb. Nutzerauthentifizierung und Durchführung von automatisierten Datenanalysen und Erstellung von Reportings. **Verarbeitung** der Daten zur	**Collection of** data through online forms, API interfaces. **Storage of** data exclusively in encrypted form in a secure cloud environment. **Use of** data to provide the service, in particular user authentication, automated data analysis and report generation. **Processing** of data to enable the

	Ermöglichung der optionalen Nutzung von KI-Funktionalitäten des Dienstes, einschließlich der Verarbeitung von KI-EIngaben und der Generierung der entsprechenden KI-Ausgaben. **Übermittlung** der Daten an Dritte (nur im Rahmen der vereinbarten Zwecke). **Löschung** der Daten nach Ablauf der Aufbewahrungsfrist oder auf Anfrage.	optional use of AI functionalities of the service, including the processing of AI inputs and the generation of corresponding AI outputs. **Transfer of** data to third parties (only for the agreed purposes). **Deletion** of data after the retention period has expired or upon request.
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	Alasco verarbeitet personenbezogene Daten im Rahmen der Erbringung ihrer Dienstleistungen zum Betrieb der SaaS-Plattform sowie zur Erfüllung der vertraglich vereinbarten Nutzungs- und Support-Services. Dies umfasst auch die Bereitstellung und Nutzung von KI-gestützten Funktionen innerhalb der Plattform. Alasco ist berechtigt, anonymisierte oder aggregierte Nutzungsdaten, einschließlich Daten über Interaktionen mit KI-Funktionen (z.B. Eingaben und Ausgaben), zu analysieren, um die Konfiguration, Benutzerfreundlichkeit und Leistungsfähigkeit ihrer Produkte und Services fortlaufend zu verbessern. Eine Weiterverarbeitung personenbezogener Daten zum Training oder zur Weiterentwicklung von KI-Modellen erfolgt nicht. Alasco handelt hierbei als Auftragsverarbeiter im Auftrag des Kunden, der für die Datenverarbeitung Verantwortlicher im Sinne der Datenschutzgesetze bleibt.	Alasco processes personal data in the course of providing its services for the operation of the SaaS platform and for the fulfillment of the contractually agreed usage and support services. This also includes the provision and use of AI-supported functions within the platform. Alasco is entitled to analyze anonymized or aggregated usage data, including data on interactions with AI functions (e.g., inputs and outputs), in order to continuously improve the configuration, user-friendliness, and performance of its products and services. Personal data is not further processed for the purpose of training or further developing AI models. Alasco acts as a processor on behalf of the customer, who remains the data controller within the meaning of data protection laws.

Dauer der Verarbeitung / Duration of the processing	Die Verarbeitungsdauer beginnt mit der Ausführung des Hauptvertrages und endet mit der Beendigung des Hauptvertrages. Die Daten werden nach Beendigung des Dienstes gelöscht, es sei denn, es bestehen gesetzliche Aufbewahrungspflichten.	The processing period begins with the execution of the main contract and ends with the termination of the main contract. The data will be deleted after the service has ended, unless there are legal storage obligations.
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	Gegenstand und Art der Verarbeitung durch unsere eingesetzten Unterauftragsverarbeiter ergibt sich aus Anhang III. Die Dauer der Verarbeitung bestimmt sich nach dem Einsatz des Unterauftragsverarbeiters in Verbindung mit der Gültigkeit des hier abgeschlossenen Vertrags. Die Verarbeitung der personenbezogenen Daten mittels KI-Diensten erfolgt ausschließlich zur Erfüllung des vertraglich vereinbarten Zwecks. Eine Nutzung der Daten für das Training, die Weiterentwicklung oder zu anderen Zwecken der zugrundeliegenden KI-Modelle ist ausgeschlossen.	The object and type of processing by our sub-processors is set out in Annex III. The duration of the processing is determined by the use of the sub-processor in conjunction with the validity of the contract concluded here. Personal data is processed using AI services exclusively for the purpose of fulfilling the contractually agreed purpose. The data may not be used for training, further development, or other purposes of the underlying AI models.

Anhang III - Technische und Organisatorische Maßnahmen
Annex III - Technical & Organisational Measures

Die technischen und organisatorischen Maßnahmen werden von Alasco in Übereinstimmung mit Art 32 Verordnung (EU) 2016/679 umgesetzt. Sie werden von Alasco entsprechend der Machbarkeit und dem Stand der Technik kontinuierlich verbessert und auf ein höheres Sicherheits- und Schutzniveau gebracht.

The technical and organisational measures are implemented by Alasco in accordance with Article 32 of Regulation (EU) 2016/679. They are continuously improved by Alasco in line with feasibility and the state of the art, and raised to a higher level of security and protection.

Alasco hat sich in seinen Richtlinien unter anderem zum Ziel gesetzt, seinen Kunden die Produkte und Dienstleistungen auf dem höchstmöglichen Niveau der Informationssicherheit in Übereinstimmung mit den Gesetzen zu liefern. Mitarbeiter von Alasco werden kontinuierlich im Bereich des Datenschutzes informiert und geschult. Darüber hinaus sind alle Mitarbeiter vertraglich auf das Datengeheimnis und die Vertraulichkeit verpflichtet. Externe Personen, die im Rahmen ihrer Tätigkeit für Alasco mit personenbezogenen Daten in Berührung kommen können, werden vor Beginn ihrer Tätigkeit mittels eines NDA (Non-Disclosure Agreement) zur Geheimhaltung und Vertraulichkeit sowie zur Einhaltung des Datenschutzes und des Datengeheimnisses verpflichtet.

Among other things, Alasco has set itself the goal in its guidelines of providing its customers with products and services at the highest possible level of information security in accordance with the law. Alasco employees receive continuous information and training in the area of data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External persons who may come into contact with personal data in the course of their work for Alasco are bound to secrecy and confidentiality as well as to compliance with data protection and data secrecy by means of an NDA (Non-Disclosure Agreement) before the start of their work.

1.	**Vertraulichkeit**	**Confidentiality**
1.1.	Physische Zugangskontrolle	Physical access control

Maßnahmen, um Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Measures to prevent unauthorised persons from accessing data processing systems that are used to process or use personal data.

- Physische Absicherung der Unternehmensräumlichkeiten, z. B. abschließbare Türen
- Verschließbare Aufbewahrungsmöglichkeiten, z. B. Schränke
- Zutrittskontrollsystem Unternehmensräumlichkeiten über elektronisches Schließsystem
- Beaufsichtigung und Begleitung von Fremdpersonen
- Kontrollierte und zentralisierte Schlüsselvergabe
- Gebäude mit Unternehmensräumlichkeiten werden durch nächtlichen Schließdienst gesichert
- Zusätzliche Absicherung kritischer Infrastruktur, z. B. abschließbare Netzwerkschränke

- Physical security of company premises, e.g. lockable doors
- Lockable storage facilities, e.g. cabinets
- Access control system for company premises via electronic locking system
- Supervision and accompaniment of external persons
- Controlled and centralised key allocation
- Company premises are secured by night-time lock service
- Additional protection of critical infrastructure, e.g. lockable network cabinets

1.2. Logische Zugangskontrolle

Logical access control

Maßnahmen um die Nutzung von Datenverarbeitungssystemen durch Unbefugte zu verhindern

Measures to prevent unauthorised usage of data processing systems

- Sichere login-Maßnahmen sind verpflichtend umgesetzt (Authentifizierung von Benutzern durch Benutzername und Passwort, wo umsetzbar technisch erzwungene Passwortkomplexität, Multifaktor Authentifizierung (MFA) wenn verfügbar)
- Zentral umgesetzte Sicherung von Endgeräten durch automatische

- Secure login measures are mandatory (authentication of users through username and password, where technically feasible enforced password complexity, multi factor authentication (MFA) where available)
- Centrally implemented security for end devices with automatic screen lock after inactivity and encryption

Bildschirmsperre von Endgeräten nach Inaktivität und Verschlüsselung
- SASE (Secure Access Service Edge) für kritische Systeme implementiert
- Web Application Firewall und technische Trennung von Netzwerken in interne und öffentlich zugängliche Netzwerke
- Zentralisiertes Zugangsmanagement für alle Systeme bei Alasco

- SASE (Secure Access Service Edge) implemented for critical systems
- Web application firewall and technical separation of networks into internal and publicly accessible networks
- Centralised access management for all systems at Alasco

1.3. Zugriffskontrolle

Maßnahmen, die sicherstellen, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Zentralisiertes Zugangsmanagement für alle Systeme bei Alasco
- Rollenvergabe über need-to-know Prinzip

Authorization control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

- Centralised access management for all systems at Alasco
- Role assignments based on need-to-know principle

1.4. Trennbarkeit

Maßnahmen, die sicherstellen, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können. Dies kann z.B. durch logische und physische Trennung der Daten gewährleistet werden.

- Technische Trennung von Produktiv- und Testsystemen
- Trennung des WLAN in privat & öffentlich

Separation Control

Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logically and physically separating the data.

- Technical separation of productive and test systems
- Separation of the WLAN into private and public

- Mandantentrennung (“multi-tenancy”) durch logische Separation - diese erfolgt auch bei der Datenabfrage und -verarbeitung im Rahmen von KI-Funktionen.
- Bei der Verarbeitung von KI-Eingaben und -Ausgaben werden zusätzlich Mechanismen zur Prompt-Sicherheit (“Prompt Injection Prevention”) implementiert, um missbräuchliche Abfragen oder die Manipulation von Daten zu verhindern.

- Tenant separation (‘multi-tenancy’) through logical separation, which also applies to data retrieval and processing within the scope of AI functions.
- When processing AI inputs and outputs, additional prompt security mechanisms (‘prompt injection prevention’) are implemented to prevent abusive queries or data manipulation.

1.5. Verschlüsselung & Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt so, dass sie ohne zusätzliche Informationen nicht mehr einer bestimmten Person zugeordnet werden können, sofern diese Informationen getrennt aufbewahrt und durch geeignete technische und organisatorische Maßnahmen geschützt sind.

- Produktivdaten werden ausschließlich anonymisiert oder pseudonymisiert auf Testsystemen verwendet
- Alle Daten, einschließlich der KI-Eingaben und KI-Ausgaben, werden ausschließlich mit state of the art Technologien verschlüsselt, gespeichert und übertragen

Encryption & Pseudonymization

Personal data is processed in such a way that it can no longer be assigned to a specific person without additional information, provided that this information is stored separately and protected by appropriate technical and organisational measures.

- Productive data is used only in anonymised or pseudonymised form on test systems.
- All data, including AI inputs and AI outputs, is stored and transmitted in encrypted form, using state-of-the-art technology.

2. Integrität

Integrity

2.1. Transport- & Übertragungskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten während der elektronischen Übermittlung oder

Transfer Control

Measures to ensure that personal data cannot be read, copied, modified or removed by unauthorised persons

während des Transports oder der Speicherung auf Datenträgern nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können und dass es möglich ist, zu überprüfen und festzustellen, an welche Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden sollen.

during electronic transmission or during transport or storage on media, and that it is possible to check and determine the places to which personal data is to be transmitted by data transmission devices.

- Systemzugriffe werden automatisch protokolliert
- Viren- und Malwareschutz durch Endpoint Detection Response System sichergestellt
- Personenbezogene Daten werden ausschließlich über verschlüsselte Verbindungen übertragen ("encryption at rest & in-transit")
- Alle Eingaben von Daten in die Alasco Applikation durchlaufen eine Firewall

- System access is automatically logged
- Virus and malware protection is ensured by the Endpoint Detection Response System
- Personal data is only transmitted via encrypted connections ('encryption at rest & in-transit')
- All data entered into the Alasco application passes through a firewall

2.2. Eingabekontrolle

Maßnahmen, die sicherstellen, dass im Nachhinein überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus ihnen entfernt worden sind. Die Eingabekontrolle erfolgt durch Protokollierung, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) erfolgen kann.

Input Control

Measures to ensure that it is possible to retrospectively review and determine whether and by whom personal data has been entered into, modified in or removed from data processing systems. Input control is carried out by means of logging, which can be done at various levels (e.g. operating system, network, firewall, database, application).

- Datenmodifikationen – einschließlich Interaktionen mit KI-Funktionen – werden in Protokollen auf Benutzerebene erfasst

- Data modifications - including interactions with AI features - are recorded in user-level logs
- Authorisation to modify personal data through central access management

- Berechtigung zum Modifizieren von personenbezogenen Daten durch zentrales Zugangsmanagement

3. Verfügbarkeit und Ausfallsicherheit

Availability and Resilience

3.1. Verfügbarkeitskontrolle

Availability

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (USV, Klimatisierung, Brandschutz, Datensicherung, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Plattenspiegelung usw.).

Measures to ensure that personal data is protected against accidental destruction or loss (uninterruptible power supply, air conditioning, fire protection, data backup, secure storage of data carriers, virus protection, RAID systems, disk mirroring, etc.).

- Hosting aller Systeme, die personenbezogene Daten verarbeiten, erfolgt ausschließlich durch zertifizierte Provider, zum Beispiel AWS. Etwaige Lieferanten werden im Beschaffungsprozess unter anderem hierauf geprüft.
- Regelmäßige Backups aller von Kunden überlassenen Daten entsprechend der Alasco Backup Policy, welche unter anderem ein multi-region Backup vorsieht
- Produktivsysteme werden in Hochverfügbarkeitsmodus gehostet, z. B. durch Nutzen aller “availability zones” von AWS

- All systems that process personal data are hosted exclusively by certified providers, such as AWS. During the procurement process, potential suppliers are checked for this, among other things.
- Regular backups of all data provided by customers in accordance with the Alasco Backup Policy, which, among other things, provides for a multi-region backup.
- Production systems are hosted in high-availability mode, e.g. by using all of AWS's ‘availability zones’.

3.2. Wiederherstellbarkeit

Recoverability

Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit von und des Zugangs zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls.

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

- Dokumentierter Disaster Recovery Plan
- Datensicherungen werden verschlüsselt und redundant (multi-region) aufbewahrt
- Einhaltung der Backup Policy wird automatisch geprüft und etwaige Verstöße automatisch an verantwortliche Personen mitgeteilt
- Regelmäßiger Test, mind. vierteljährlich, des Disaster Recovery Plans, der die Les- und Nutzbarkeit der Backups inkludiert
- Ergebnisse der Recovery Tests werden dokumentiert und an das Management-Team berichtet. In Bezug auf identifizierte Schwachstellen werden zeitnah Korrekturmaßnahmen eingeleitet, deren Umsetzung kontinuierlich nachverfolgt wird

- Documented disaster recovery plan
- Data backups are encrypted and stored redundantly (multi-region)
- Compliance with the backup policy is automatically checked and any violations are automatically reported to the responsible persons
- Regular testing, at least quarterly, of the disaster recovery plan, which includes the readability and usability of the backups
- The results of the recovery tests are documented and reported to the management team. With regard to identified weaknesses, corrective measures are initiated in a timely manner and their implementation is continuously monitored.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4. Procedure for regular review, assessment and evaluation

4.1. Datenschutzmanagement

Maßnahmen zur laufenden Überwachung und Steuerung des Umgangs mit personenbezogenen Daten, einschließlich regelmäßiger Audits, Schulungen und der Dokumentation von Datenschutzvorfällen

- Technische und organisatorische Maßnahmen werden durchgehend, jedoch mindestens jährlich, auf Effektivität geprüft und entsprechend angepasst
- Datenschutzbeauftragter ist bestellt

Data protection management

Measures for the ongoing monitoring and control of the handling of personal data, including regular audits, training and the documentation of data breaches.

- Technical and organisational measures are continuously, but at least annually, reviewed for effectiveness and adjusted accordingly.

- Mindestens jährliche Datenschutz- und IT-Sicherheitssensibilisierung für alle Mitarbeiter verpflichtend
- Datenschutz ist Teil des Alasco Risikomanagementprozess

- A data protection officer has been appointed.
- At least annual data protection and IT security awareness training is mandatory for all employees.
- Data protection is part of the Alasco risk management process.

4.2. Incident-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen und bei der Bearbeitung von Datenpannen.

- Festgelegter "Incident Response Prozess" (IR Prozess) zur Sicherstellung der schnellstmöglichen Wiederherstellung des Service, Lösung etwaiger Probleme und Information relevanter Stakeholder.
- IR Prozess definiert Rollen, Verantwortliche und Aufgaben
- IR Prozess inkludiert eine regelmäßige Evaluation des Prozesses selbst sowie anhängender Prozesse & Systeme

Incident management

Support in responding to security breaches and handling data incidents.

- Defined 'incident response process' (IR process) to ensure the fastest possible recovery of the service, resolution of any issues and information to relevant stakeholders.
- IR process defines roles, responsibilities and tasks
- IR process includes regular evaluation of the process itself and of attached processes & systems

4.3. Datenschutz by Design

Maßnahmen gemäß Artikel 25 der Verordnung (EU) 2016/679, die den Grundsätzen des Datenschutzes durch Technik und durch Voreinstellungen entsprechen.

- Das Prinzip der „Privacy by Default" wird durch technische Standardeinstellungen gewährleistet, die es dem Benutzer ermöglichen, die Datenfreigabe, auch bei der Nutzung des KI-Assistenten, auf das notwendige Minimum zu beschränken.

Data protection by design

Measures in accordance with Article 25 of Regulation (EU) 2016/679, which are in line with the principles of data protection by design and by default.

- The principle of 'Privacy by Default' is implemented through technical standard settings that enable the user, also when using the AI assistant, to restrict the sharing of data to the necessary minimum.
- Collection of personal data only to the extent necessary for the respective purpose

- Sammlung von persönlichen Daten nur in einem Umfang, der im Rahmen des jeweiligen Verwendungszweckes nötig ist.
- Alasco gewährleistet, dass Nutzer beim Einsatz des KI-Assistenten einen klaren Hinweis darüber erhalten, dass sie mit einem KI-System interagieren (Transparenzpflicht nach Art. 50 AI Act). Zudem wird den Nutzern ein Opt-out von der Nutzung des KI-Assistenten ermöglicht.

- Alasco ensures that users are clearly informed when using the AI assistant that they are interacting with an AI system (transparency requirement under Section 50 of the AI Act). Users are also given the option to opt out of using the AI assistant.

4.4. Auftragskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, nur gemäß den Anweisungen des Kunden verarbeitet werden können.

Sorgfältige Lieferantenauswahl, in Zusammenarbeit mit Security Board & Rechtsabteilung nach festgelegten Kriterien, insbesondere hinsichtlich Datenschutz und IT-Sicherheit, insbesondere Prüfung der Dokumentation und Einhaltung der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO

- Im Rahmen des Prozesses wird eine Risikobewertung für die jeweiligen Lieferanten durchgeführt, sofern der Drittanbieter regelmäßig mit personenbezogenen Daten arbeitet
- Externe KI-Dienstleister (Unterauftragsverarbeiter) werden nur nach Freigabe durch den Verantwortlichen und unter Einhaltung der Anforderungen nach Art. 28 DSGVO eingesetzt.

Order control

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the customer's instructions.

Careful selection of suppliers, in cooperation with the security board and legal department, according to defined criteria, in particular with regard to data protection and IT security, in particular checking documentation and compliance with the technical and organisational measures according to Art. 32 GDPR

- As part of the process, a risk assessment is carried out for the respective suppliers if the third-party provider regularly works with personal data.
- External AI service providers (subprocessors) are only used after approval by the controller and in compliance with the requirements of Art. 28 GDPR.
- The processor shall contractually oblige its subprocessors not to use

- Der Auftragsverarbeiter verpflichtet seine Unterauftragsverarbeiter vertraglich, dass die im Rahmen dieses Vertrages verarbeiteten personenbezogenen Daten nicht zum Training, zur Verbesserung oder zu sonstigen zweckfremden Zwecken der KI-Modelle verwendet werden.
- Alasco überzeugt sich von der Einhaltung der technischen und organisatorischen Maßnahmen durch die beauftragten Unterauftragsverarbeiter sowohl vor Aufnahme der Tätigkeit als auch in regelmäßigen Abständen danach.

the personal data processed under this contract for training, improving, or other purposes unrelated to the AI models.
- Alasco ensures that the subcontractors used comply with the technical and organisational measures before the start of the assignment and regularly thereafter.

Anhang IV - Liste der Unterauftragnehmer
Annex IV - List of subprocessors

- s. List of subprocessors -

https://www.alasco.com/legal/list-of-sub-processors