Auftragsverarbeitungsvertrag der neurocat GmbH

(Stand: August 2023)

Präambel: Dieser Vertrag regelt die Rechtsbeziehungen der neurocat GmbH (nachfolgend „Auftragsverarbeiter“) und ihren Unternehmenskund:innen (nachfolgend „Auftraggeber“) bei der Nutzung einer vom Auftragsverarbeiter betriebenen Software. Hierbei sind die Vertragsparteien mit der neurocat Lizenzvereinbarung für Endanwender:innen und/oder der neurocat Lizenzvereinbarung für Endanwender:innen der Demolizenz (nachfolgend „Hauptvertrag“) ein Auftragsverarbeitungsverhältnis (nachfolgend „Auftrag“) eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (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 - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien den nachfolgenden Vertrag.

§ 1 Anwendungsbereich

Dieser Vertrag findet Anwendung auf die nach Art. 4 Abs. 2 DSGVO definierte Verarbeitung („Verarbeitung“) aller nach Art. 4 Abs. 1 DSGVO definierten personenbezogenen Daten, für die der Auftraggeber als nach Art. 4 Abs. 7 DSGVO definierte/r Verantwortliche:r im Sinne der datenschutz-rechtlichen Vorschriften fungiert („Verantwortlicher“) , die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden („Daten“).

§ 2 Konkretisierung des Auftragsinhaltes

(1) Der Auftragsverarbeiter verarbeitet die Daten im Auftrag und nach Weisung des Auftraggebers im Sinne des Art. DSGVO („Auftragsverarbeitung“). Der Auftraggeber bleibt im datenschutzrechtlichen Sinne Verantwortlicher.

(2) Gegenstand der der Auftragsverarbeitung, Art und Zweck der vorgesehenen Verarbeitung von Daten sowie die Kategorien der von der Verarbeitung im Rahmen dieses Auftrags betroffenen Personen („Betroffene“) bestimmen sich nach Anlage 1.

Data Processing Agreement of the neurocat GmbH

(Last updated: August 2023)

Preamble: This Agreement governs the legal relationship between neurocat GmbH (hereinafter referred to as the "Data Processor") and its corporate clients (hereinafter referred to as the "Contracting Parties") in the use of software operated by the Data Processor. With the neurocat license agreement for end users, the Contracting Parties have entered into a data processing relationship (hereinafter referred to as "DPR") The Contracting Parties enter into the following agreement in order to define the resulting rights and obligations in accordance with the requirements of the European General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016 concerning the protection of individuals with regard to processing personal data, the free movement of said data and the repeal of Directive 95/46/EC – GDPR) and the German Federal Data Protection Act (BDSG).

§ 1 Scope

This Agreement applies to the processing as defined in Art. 4 (2) GDPR ("Processing") of all personal data as defined in Art. 4 (1) GDPR for which the Contracting Party is the Controller within the meaning of Art. 4 (7) GDPR ("Controller") which is the subject of the Service Agreement or which arises in the course of its performance or which becomes known to the Data Processor ("Data").

§ 2 Substantiation of the contents of the order

(1) The Data Processor processes the data on behalf of and according to the instructions of the Contracting Party within the meaning of Art. 28 GDPR (Data Processing). The Contracting Party remains the Data Controller in terms of data protection law.

(2) The object of the order processing, the nature and purpose of the intended data processing and the categories of Data Subject ("Data Subject") affected by the processing in the context of this order are defined in accordance with Annex 1.

(3) Die Dauer dieses Auftrags entspricht der Laufzeit des der Verarbeitung zugrundeliegenden Auftrags-verhältnisses. Die Regelungen zur ordentlichen Kündigung des Hauptvertrages gelten entsprechend. Eine Kündigung des Hauptvertrages bewirkt automatisch die Kündigung dieses Vertrages. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragsverarbeiter ander-weitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftrags-verarbeitung vorrangig gelten, sofern die Parteien nicht ausdrücklich etwas anderes vereinbart haben.

§ 3 Verantwortlichkeit des Auftragsgeber

(1) Der Der Auftraggeber ist für die Beurteilung der Zulässigkeit der Datenverarbeitung nach Art. 6 Abs. 1 DSGVO und für die Wahrung der Rechte der Betroffenen nach Art. 12 ff. DSGVO verantwortlich.

(2) Stellt der Auftraggeber bei der Prüfung der Auftragsergebnisse des Auftragsverarbeiters Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Vorschriften oder seine Weisungen fest, hat er den Auftragsverarbeiter unverzüglich und umfassend über diese zu informieren.

§ 4 Verantwortlichkeit des Auftragsverarbeiters

(1) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsver-arbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter tech-nischer und organisatorischer Maßnahmen (vgl. § 8). Darüber hinaus unterstützen sich die Vertrags-parteien gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechen-schaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO).

(2) Der Auftragsverarbeiter hat dem Auftraggeber auf sein Verlangen hin jederzeit die Daten heraus-zugeben, zu berichtigen, anzupassen, zu löschen oder deren Verarbeitung einzuschränken.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird dieser das Ersuchen unverzüglich an den

(3) The duration of this DPR corresponds to the duration of the contractual relationship that underlies the processing. The provisions concerning ordinary termination of the Main Agreement apply mutatis mutandis. Termination of the Main Agreement automatically results in termination of this Agreement. Isolated termination of this Agreement is excluded.

(4) Insofaras other agreements between the Contracting Party and the Data Processor provide for other agreements on the protection of personal data, this Data Processing Agreement takes precedence, unless the Parties have expressly agreed otherwise.

§ 3 Responsibility of the Contracting Party

(1) The Contracting Party is responsible for assessing the permissibility of data processing pursuant to Art. 6 (1) GDPR and for safeguarding the rights of the Data Subjects pursuant to Art. 12 et seq. GDPR.

(2) If the Contracting Party identifies errors or irregularities concerning data protection regulations or their instructions while reviewing the processing results obtained by the Data Processor, they are to inform the Data Processor of these immediately and in full.

§ 4 Responsibility of the Data Processor

(1) A To safeguard the protection of Data Subjects' rights, the Data Processor will provide the Data Controller with adequate support, in particular by ensuring the adoption of appropriate technical and organisational measures (cf. Sec. 8). Moreover, the Contracting Parties support each other in demonstrating and documenting the accountability incumbent upon them with regard to the principles of proper data processing (Art. 5 (2), Art. 24 (1) GDPR).

(2) At the Contracting Party's request, the Data Processor is obliged at any time to surrender, correct, adapt, delete or restrict processing of the data.

(3) If a Data Subject contacts the Data Processor directly for the purpose of asserting a Data Subject's right, the Data Processor will forward the request to the Data Controller without delay.

Verantwortlichen weiterleiten.

(4) (Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maß-nahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen der Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Weisungsgebundenheit des Auftragsverarbeiters

(1) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch Gesetz oder durch Anordnung einer staatlichen Stelle innerhalb der Grenzen der DSGVO hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, er-gänzt oder ersetzt werden. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Angebot auf Leistungsänderung behandelt. Weisungen vom Auftraggeber an den Auftragsverarbeiter sind an die E-Mail dataprivacy@neurocat.ai zu richten.

(3) Die weisungsberechtigten Personen des Auftragsverarbeiters sind die Geschäftsführung und Prokuristen des Auftragsverarbeiters.

§ 6 Datenverarbeitung

(1) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam zwischen Auftragsverarbeiter und Auftraggeber abzustimmen und zu dokumentieren. Auskünfte an Dritte oder an die betroffene Person darf der

(4) The Data Processor informs the Data Controller without undue delay of inspections and measures undertaken by supervisory authorities or if a supervisory authority inquires, investigates or otherwise makes enquiries of the Data Processor within the scope of their authority.

§ 5 Obligation of the Data Processor to follow instructions

(1) The Data Processor is only permitted to process data in accordance with the instructions given by the Data Controller, unless they are obliged to do so by law or by order of a government agency within the limits of the GDPR (e.g. investigations by law enforcement or national security agencies). In such a case, the data Processor will notify the Data Controller of these legal requirements prior to processing, unless the law in question prohibits such a notification owing to an important public interest (Art. 28 (3) (2) (a) GDPR).

(2) An instruction is the written, electronic or verbal order issued by the Data Controller for the Data Processor to handle data in a specific way. Such orders are to be documented. The instructions are initially defined by the service agreement and can subsequently be amended, supplemented or replaced by the Data Controller in documented form by means of an individual instruction. Instructions that go beyond the service agreed in the Main Agreement will be treated as an offer to amend the service. Instructions from the Contracting Party to the Data Processor are to be sent to the email: dataprivacy@neurocat.ai.

(3) The persons authorised to give instructions at the Data Processor are the management and the authorised signatories at the Data Processor.

§ 6 Data Processing

(1) Changes to the object of processing that involve process changes are to be jointly agreed and documented. The Data Processor is only permitted to provide information to third parties or the Data Subject with the prior express written

Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Auftraggeber erteilen.

(2) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(3) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet auf dem Gebiet der Europäischen Union statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig, wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen. Die grundlegenden Voraus-setzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(4) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur mit Zustimmung des Verantwortlichen verarbeiten.

§ 7 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

§ 8 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in der Anlage 2 zu diesem Vertrag niedergelegten

consent of the Data Controller. The Data Processor uses the data exclusively for statistical purposes and for the further development of the software provided. They are not entitled to pass the data on to third parties.

(2) The Data Controller is responsible for keeping a register of processing operations within the meaning of Art. 30 (1) GDPR. The Data Processor will supply the Data Controller with information for inclusion in the directory at the Data Controller's request. The Data Processor will maintain a register of all categories of processing operation carried out on behalf of the Data Controller in accordance with the requirements of Art. 30 (2) GDPR.

(3) Data processing performed on behalf of the Data Controller will take place within the territory of the European Union. Processing in a state outside the territory referred to in the Sentence 1 is only permitted if safeguards ensure that the level of protection guaranteed by the GDPR taking into account the requirements of Chapter V GDPR is not undermined and requires the prior express written consent of the Data Controller. The basic conditions for the lawfulness of such processing remain unaffected.

(4) The Data Processor will ensure that natural persons under their authority who have access to data only process it when instructed to do so by the Data Controller. The processing of data outside the Data Processor's premises may only be carried out if appropriate technical and organisational measures to secure the processing environment are put into place.

§ 7 Compliance by the Data Processor with mandatory legal obligations

The Data Processor ensures that the persons authorised to process the data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality and provide evidence of this to the Data Controller on request. This also includes the briefing about the obligation to give instructions and the limitation in purpose that exists in this Data Processing Relationship.

§ 8 Technical and organisational measures and their control

(1) The Contracting Parties agree on the specific technical and organisational safeguards set out in

konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieses Vertrages.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maß-nahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in diesem Vertrag getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die von dem Verant-wortlichen oder einem/einer anderen von diesem beauftragten Prüfer:in durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer:innen, unabhängige Datenschutzauditor:innen), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch einen IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 DSGVO und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsver-arbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach vorheriger Anmeldung, sofern nicht ein Zugang ohne Anmeldung erforderlich ist, von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen. Der Auftragsverarbeiter verpflichtet sich zur Erfüllung seiner jeweiligen gesetzlich zugewiesenen Verpflichtungen gegenüber dem/der

Annex 2 to this Agreement. The Annex forms an integral part of this Agreement.

(2) Technical and organisational measures are subject to technical advancement. The Data Processor is allowed to implement adequate alternative measures in this context. The safeguarding level for the measures specified in the Annex "Technical and organisational measures" is not allowed to be undercut thereby. Significant changes are to be documented.

(3) The Data Processor will provide the Data Controller with all the information required to demonstrate compliance with the provisions of this Agreement and those of the law. In particular, they will facilitate reviews/inspections undertaken by the Data Controller or another auditor appointed by the Data Controller and assist in their completion. Verification of the implementation of such measures, which do not only relate to the specific order, can also be provided by submitting a current audit certificate, through reports from sufficiently qualified and independent bodies (e.g. auditors, independent data protection auditors), by complying with approved codes of conduct in accordance with Art. 40 GDPR, through certification in accordance with Art. 42 GDPR or through suitable certification by an IT security or data protection audit (e.g. in accordance with BSI baseline protection). The Data Processor undertakes to inform the Data Controller without undue delay of the exclusion of approved codes of conduct pursuant to Art. 41 (4) GDPR, the revocation of a certificate pursuant to Art. 42 (7) and any other form of withdrawal or material change in the aforementioned verifications.

(4) The Data Controller is entitled to inspect the adequacy of the measures taken to comply with the legal or technical and organisational requirements necessary for implementing this Agreement at any time for inspection purposes at the Processor's premises during normal business hours without disrupting operations, subject to prior notification, unless access without notification appears necessary.

Datenschutzbeauftragten des Verantwortlichen sowie der zuständigen Aufsichtsbehörde.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus die erforderlichen Informationen, insbesondere die technischen und organisatorischen Maßnahmen sowie sonstige Dokumentationen von datenschutzbezogenen Prozessen zur Verfügung, die er für die Prüfungen nach Absatz 4 benötigt.

(6) Der Auftragsverarbeiter hat im Einvernehmen mit dem/der Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. zur Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 9 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Im Hinblick auf die Meldepflicht nach Art. 33 Abs. 3 DSGVO und die korrespondierende Pflicht des Verantwortlichen nach Art. 33 und Art. 34 DSGVO, verpflichtet sich der Auftragsverarbeiter den Verantwortlichen umgehend zu unterrichten, insbesondere
(a) bei schwerwiegenden Störungen seines Betriebsablaufs;
(b) bei Verdacht auf Verstöße gegen diesen Vertrag;
(c) bei Verdacht auf Verstöße gegen gesetzliche Datenschutzbestimmungen;
(d) bei Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen.
Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen und ihm in diesem Zusammenhang auf Anfrage sämtliche relevanten Informationen zur Verfügung zu stellen.

§ 10 Löschung und Rückgabe von Daten

(1) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens, wenn nach hinreichender Wahrscheinlichkeit mit Beendigung der Leistungsvereinbarung keine nachvertraglichen Ansprüche mehr in Betracht kommen, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des

(5) The Data Processor will also supply the Data Controller with all the information required to carry out the inspections referred to under (4).

(6) In consultation with the Data Controller, the Data Processor will take all necessary measures to backup the data or safeguard its processing, also specifically taking into account the state of the art, as well as mitigate any possible adverse consequences for Data Subjects.

§ 9 Notification of breaches by the Data Processor

With regard to the notification obligation pursuant to Art. 33 (3) GDPR and the corresponding obligation of the Data Controller pursuant to Art. 33 and Art. 34 GDPR, the Data Processor undertakes to inform the Data Controller without delay, in particular
a) In the event of serious disruptions to their operations,
b) If there is a suspicion of breaches of this Agreement,
c) If there is a suspicion of breaches of statutory data protection regulations and
d) In the event of irregularities in processing data by the Data Controller.
The Data Processor undertakes to provide the Data Controller with reasonable assistance, where necessary, in fulfilling their obligations under Art. 33 and 34 GDPR and, in this context, to furnish the Data Processor with all relevant information upon request.

§ 10 Deletion and return of data

(1) On completion of the contractually agreed services or earlier at the request of the Data Controller, but no later than when it is reasonably probable that post-contractual claims cease to apply on termination of the Service agreement, the Processor will surrender to the Data Controller or, with the prior consent of the Data Controller, destroy in accordance with data protection law, all documents, processing and exploitation results and data files (as well as copies or reproductions thereof) that have come into their possession and that relate to the contractual relationship. The same applies to test and reject material. This does not apply to data

Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Davon ausgenommen sind Daten, welche zu Beweiszwecken für einen juristischen Prozess unveränderlich gesichert werden müssen („Litigation Hold“).

that needs to be preserved in an unalterable form as evidence for litigation purposes ("litigation hold").

(2) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend den jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 1.

(2) The Data Processor can retain documents which serve as proof of the orderly and proper processing of data in accordance with the respective retention periods until the end thereof, even beyond the end of the Agreement. Alternatively, they can hand over these documents to the Data Controller at the end of the Agreement to discharge themselves from any further responsibility. The obligations under (1) applies to the data retained in accordance with (1) after the end of the retention period.

§ 11 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieses Vertrages sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Zur Durchführung solcher Dienstleistungen beauftragt der Auftragsverarbeiter entsprechende Dienstleister ("Unterauftragsverarbeiter"). Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. in Form von Telekommunikationsleistungen zur Unterstützung der Hauptleistung in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

§ 11 Subcontracting Relationships

(1) In terms of this Agreement, subcontracting relationships are to be understood to mean services that directly relate to the provision of the main service. This does not include ancillary services used by the Data Processor, e.g. in the form of telecommunication services or disposing of data carriers, in support of the main service. However, in the case of ancillary services outsourced to third parties, the Data Processor is also obliged to enter into appropriate and legally compliant contractual agreements and control measures to guarantee the data protection and security of the Contracting Party's data.

(2) Der Auftragsverarbeiter ist berechtigt, zur Durchführung des Auftrags die in Anlage 3 aufgeführten Unterauftragsverarbeiter zur Verarbeitung personenbezogener Daten einzusetzen. Die Beauftragung weiterer oder anderer Unterauftragsverarbeiter zur Verarbeitung personenbezogener Daten des Auftraggebers ist nur nach vorheriger schriftlicher Information des Auftragsverarbeiters über die Identität des Unterauftragsverarbeiters und den Gegenstand des Unterauftrags zulässig, sofern der Auftraggeber dieser Änderung nicht innerhalb einer angemessenen Frist von 14 Werktagen widerspricht.

(2) The Data Processor is entitled to deploy the sub-processors listed in Annex 3 to process personal data in order to complete the order. Commissioning additional or other sub-processors to process personal data belonging to the Contracting Party is only permitted after the Data Processor has provided prior written information about the identity of the sub-processor and the subject of the sub-processing activity, unless the Contracting Party objects to this change within a reasonable period of at least 14 working days.

(3) Im Übrigen gelten die folgenden

(3) Otherwise, the following requirements apply to

Voraussetzungen für die Begründung und Aufrechterhaltung von Unterauftragsverhältnissen:

(a) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unter-beauftragung gestattet.

(b) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung mit Zustimmung des Auftraggebers außerhalb der EU, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit nach Maßgabe der für die Durchführung des Auftrags geltenden datenschutzrechtlichen Vorschriften sicher. Dies gilt auch für den Fall des Einsatzes eines/einer Dienstleisters/Dienstleisterin im Sinne des § 11 Abs. 1 Satz 2.

(c) Dem Unterauftragsverarbeiter sind im Wege eines Vertrages dieselben Datenschutzpflichten aufzu-erlegen, die in diesem Vertrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt.

(d) Der Verantwortliche ist ebenso berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Aus-kunft über den Inhalt des mit dem Unterauftragsverarbeiter geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragsverarbeiters zu erhalten.

(e) Kommt der Unterauftragsverarbeiter seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verant-wortlichen die Beschäftigung des Unterauftragsverarbeiters ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Unterauftragsverarbeiter zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 12 Anfragen und Rechte betroffener Personen

(1) Der Auftragsverarbeiter unterstützt den

establishing and maintaining subcontracting relationships:

(a) The transfer to the sub-processor of personal data belonging to the Contracting Party and the sub-processor's initial activities are only permitted once all the conditions for subcontracting have been met.

(b) If the sub-processor renders the agreed service outside the EU with the consent of the Contracting Party, the Data Processor will ensure that this is admissible under data protection law in accordance with the provisions of data protection law applicable to completion of the order. This also applies in the case of deploying a service provider within the meaning of Sec. 8 (1) (2).

(c) The same data protection obligations as set out in this Agreement will be imposed upon the sub-processor by means of an agreement, whereby in particular sufficient guarantees will have to be provided to ensure that the appropriate technical and organisational measures will be implemented so that processing will be carried out in accordance with the legal requirements.

(d) On written request, the Data Controller is also entitled to receive information from the Data Processor concerning the content of the agreement concluded with the subcontractor and the fulfilment of the subcontractor's data protection obligations contained therein.

(e) If the sub-processor fails to comply with their obligations under data protection law, the Data Processor is liable to the Data Controller for complying with the sub-processor's obligations. In this case, at the request of the Data Controller, the Data Processor will terminate the engagement of the subcontractor either in whole or in part or dissolve the contractual relationship with them if and to the extent that this is not disproportionate.

§ 12 Requests and rights of Data Subjects

(1) The Data Processor shall, to the extent possible,

Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von seinen Pflichten nach Art. 12-22 sowie 32 und 36 DSGVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner/ihrer Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 13 Haftung

Die Haftung des Auftragsverarbeiters gegenüber dem/der Verantwortlichen für schuldhafte Verletzungen dieses Vertrags bestimmt sich nach den gesetzlichen Vorschriften. Der Auftragsverarbeiter haftet nicht, sofern er bei Erhebung bzw. Verarbeitung der Daten die Regelungen dieses Vertrags beachtet hat und insbesondere die technischen und organisatorischen Sicherheitsmaßnahmen wie vereinbart umgesetzt hat.

§ 14 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung und des ausdrück-lichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieses Vertrages unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder un-durchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

(3) Im Fall von Widersprüchen und Auslegungsfragen zwischen der deutschsprachigen und der englischsprachigen Fassung hat die deutschsprachige Fassung Vorrang. Im Streitfall ist allein die deutsche Fassung verbindlich.

take appropriate technical and organisational measures to assist the Contracting Party in fulfilling its obligations under Art. 12-22 and 32 and 36 GDPR.

(2) If a Data Subject asserts rights directly against the Data Processor, such as the right of access, rectification or erasure of his/her data, the Data Processor shall not respond independently but shall refer the Data Subject without undue delay to the Contracting Party and await the instructions of the Contracting Party.

§ 11 Liability

The liability of the Data Processor towards the Data Controller for culpable breaches of this Agreement are determined in accordance with the statutory provisions. The Data Processor bears no liability insofar as they have complied with the provisions of this Agreement when collecting or processing the data and, in particular, if they have implemented the technical and organisational safeguards as agreed.

§ 14 Final Provisions

(1) Amendments and supplements to this Annex and all its components – including any undertakings provided by the Data Processor – require written agreement and express reference to the fact that an amendment or supplement to these conditions are concerned. This also applies to a waiver of this written form requirement.

(2) If any of the provisions of this Agreement are invalid or unenforceable, it does affect the validity of the remaining provisions. The invalid or unenforceable provision will be replaced by a valid and enforceable provision that comes closest to the impacts of the objective that the Parties pursued with the invalid or unenforceable provision. The aforementioned provisions apply in the event that the Agreement proves to be incomplete.

(3) In the event of inconsistencies or questions of interpretation between the German and English versions, the German version prevails. Only the German version is binding in the event of a dispute

Anlage 1 – Art und Umfang der Datenverarbeitung, Kategorien der Daten und der Betroffenen

a) Art der Verarbeitung (Art. 4 Abs. 2 DSGVO):

Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung.

Im Rahmen der konkret vorliegenden Auftragsverarbeitung werden insbesondere Bilddaten, Radardaten und Lidardaten gespeichert, verarbeitet und analysiert. Ferner finden Fernwartungen und First-Level-Support bei der Anwendung der Software statt. Weiteres ergibt sich aus dem Hauptvertrag und der jeweiligen Bestellung.

b) Namen und Kontaktdaten (Art. 30 Abs. 2 lit. A DSGVO):

Kontaktdaten des Auftragsverarbeiters:

neurocat GmbH
Geschäftsführung Florens Greßner
Rudower Chaussee 29, 12489 Berlin, Deutschland
Tel.: +49 30 34065918
E-Mail: info@neurocat.ai

Derzeit ist als externe Datenschutzbeauftragte beim Auftragsverarbeiter bestellt:

Jacqueline Vogel
Datenschutzauditor (TÜV)
Firma TENCOS IT+Datenschutz
Haßbergstraße 1, 97532 Üchtelhausen, Deutschland
Tel.: +49 (0) 9724 90 76 506
E-Mail: j.vogel@tencos.de

c) Kategorien personenbezogener Daten (Art. 30 Abs. 2 lit. B DSGVO):

- Technische Daten (z.B. IP-Adresse, Gerät, Browser, Standort, Mac-Adresse, Produktversion, Logdaten)
- Bilddaten (z.B. Verkehrsbilder, annotierte Daten)
- Modelldaten (z.B. aus KI-Frameworks exportierte Modelle, ausführbarer Code, Gewichtungen)
- Metadaten (z.B. Geodaten, Bildnamen, Zeitdaten)
- Sensordaten (z.B. Radar- und Lidardaten)

Es werden keine personenbezogenen Daten der besonderen Kategorie verarbeitet.

d) Kategorien betroffener Personen (Art. 4 Nr. 1 DSGVO):

- Mitarbeiter:innen des Kunden (z.B. Ansprechpartner, Endanwender der Software)

Annex 1 – Purpose, type and scope of data processing, type of data and group of data subjects

a) Type of processing (Art. 4 (2) GDPR)

Collection, recording, receipt, arrangement, storage, adaptation or alteration, read-out, retrieval, use, disclosure by transfer, dissemination or any other form of rendering available, matching or linking, restriction, updating, deletion or destruction.

As part of the actual order processing, image data, radar data and lidar data are stored, processed and analysed. In addition, remote maintenance and first-level support are provided for the use of the software. Further details are set out in the main contract and the relevant order.
The foregoing list outlines the processing activities that may be performed as a part of the service and the type of personal data involved:

b) Names and contact details (Art. 30 (2) A GDPR):

Data Processor's contact details:

neurocat GmbH
Chief Executive Officer: Florens Greßner
Rudower Chaussee 29, 12489 Berlin, Germany
Phone: +49 30 34065918
Email: info@neurocat.ai

Currently appointed as external data protection officer at the Data Processor:

Jacqueline Vogel
Data Protection Auditor (TÜV)
TENCOS IT+Datenschutz
Haßbergstraße 1, 97532 Üchtelhausen, Germany
Phone: +49 (0) 9724 90 76 506
Email: j.vogel@tencos.de

c) Categories of personal data (Art. 30 (2) B GDPR):

- Technical data (e.g. IP address, device, browser, location, Mac address, product version, log data)
- Image data (e.g. traffic images, annotated data)
- Model data (e.g. models exported from AI frameworks, executable code, quantifiers)
- Metadata (e.g. geodata, image names, time data)
- Sensor data (e.g. radar and lidar data)

No special category personal data is processed.

d) Categories of Data Subject (Art. 4 (1) GDPR):

- The client's employees (e.g. contact persons, end users of the software)
- Other road users (e.g. vehicles, pedestrians, cyclists,

· Andere Verkehrsteilnehmer (z.B. Fahrzeuge, Fußgänger, Radfahrer, Autofahrer)

e) Kategorien von Empfängern
· Amazon Web Services (AWS)

f) Übermittlungen in Drittländer

Die Auftragsverarbeitung erfolgt innerhalb der EU oder des EWR. Es werden keine Übermittlungen in Drittländer vorgenommen.

motorists)

e) Categories of recipients
· Amazon Web Services (AWS)

f) Transfers to third countries

Order processing takes place inside the EU or EEA. Transfers to third countries do not take place.

Anlage 2 – Technische und organisatorische Maßnahmen

Vom Auftragsverarbeiter zugesicherte und umgesetzte technische und organisatorische Maßnahmen (Art. 30 Abs. 2 lit. d DSGVO):
a) Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle Kein unbefugter Zutritt zu den Datenverarbeitungs-anlagen	**Sicherheitsvorkehrungen am Gebäude der neurocat GmbH**		**Sicherheitsvorkehrungen am Serverstandort von Amazon Web Services EMEA SARL**	
	Transponder	(+)	Schlüssel	(+)
	Magnet- oder Chipkarte		Magnet- oder Chipkarte	(+)
	Elektrische Tür-öffner	(+)	Elektrische Tür-öffner	(+)
	Alarmanlage		Alarmanlage	(+)
	Videoanlage		Videoanlage	(+)
	Zaun		Zaun	(+)
	Werkschutz		Werkschutz	(+)
	Empfang	(+)	Empfang	(+)

Zugangskontrolle Kein unbefugter Zugang in Datenverarbeitungs-systeme – EDV	Sichere Passwörter	(+)
	Automatische Sperrmechanismen	(+)
	Zwei-Faktor-Authentisierung	(+)
	Verschlüsselung von Datenträgern	(+)

Zugriffskontrolle Innerhalb des Systems kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen – EDV	Berechtigungskonzepte/ Bedarfsgerechte Zugriffsrechte	(+)
	Protokollierung von Zugriffen	(+)

Annex 2 – Technical and organisational measures

Technical and organisational measures implemented and warranted by the Data Processor:
a) Confidentiality (Art. 32 (1) (b) GDPR)

Access Control No unauthorised access to the data processing systems	**Security precautions in the neurocat GmbH building**		**Security precautions at the server location of Amazon Web Services EMEA SARL**	
	Transponder	(+)	Key	(+)
	Magnetic or chip card		Magnetic or chip card	(+)
	Electric door openers	(+)	Electric door openers	(+)
	Alarm system		Alarm system	(+)
	Video system	(+)	Video system	(+)
	Fence		Fence	(+)
	On-site security		On-site security	(+)
	Reception	(+)	Reception	(+)

Access Control No unauthorised access to data processing systems – IT	Secure passwords	(+)
	Automatic locking mechanisms	(+)
	Two-factor authentication	(+)
	Encryption of data media on laptops/notebooks	(+)

Access Control No unauthorised reading, copying, modification or removal within the system – IT	Authorisation concepts/needs-based access rights	(+)
	Logging of access	(+)

Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden – EDV	Sandboxing (Bearbeitung in isolierten Bereichen)	(+)

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

Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung und Transport - EDV	Verschlüsselung	(+)
	Virtual Private Networks (VPN)	(+)
Eingabekontrolle Wann wurde welche Angabe wo eingegeben, verändert oder entfernt?	Protokollierung	(+)
	Dokumentationsmanagement	(+)

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

Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung oder Verlust	Backup – Strategie online/offline, onsite/offsite	(+)
	Unterbrechungsfreie Stromversorgung	(+)
	Virenschutz	(+)
	Firewall	(+)
	Meldewege und Notfallpläne	(+)
	Rasche Wiederherstellbarkeit	(+)

Separation Control Separate processing of data collected for different purposes – IT	Sandboxing (processing in isolated areas)	(+)

b) Integrity (Art. 32 (1) (b) GDPR)

Disclosure Control No unauthorised reading, copying, changing or removal during electronic data transfer and transportation – IT	Encryption	(+)
	Virtual Private Networks (VPN)	(+)
Input Control When and where was what information entered, changed or removed?	Logging	(+)
	Documentation management	(+)

c) Availability and resilience (Art. 32 (1) (b) & (c) GDPR)

Availability Control Protection against accidental or deliberate destruction or loss	Backup strategy online/offline, on-site/off-site	(+)
	Uninterrupted Power Supply (UPS)	(+)
	Anti-virus protection	(+)
	Firewall	(+)
	Reporting channels and emergency plans	(+)
	Rapid recoverability	(+)

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

Datenschutzmanagement	Datenschutzbeauftragte (Jaqueline Vogel, TENCOS - IT + Datenschutz) -Dokumentation der Richtlinien zum Datenschutz -Datenschutzkonzept	(+)
Incident-Response-Management (IRM) Im Falle der Verletzung des Schutzes personenbezogener Daten liegt ein dokumentierter Prozess vor, der das Vorgehen genau beschreibt, um die daraus resultierenden Risiken zu minimieren. Dazu zählen insbesondere die geltenden Meldepflichten und -fristen sowie die zur Meldung notwendigen Kontaktdaten und Prozesse.		(+)
Auftragskontrolle Keine Auftragsverarbeitung ohne Weisung des Auftraggebers	Eindeutige Vertragsgestaltung	(+)
	Formalisiertes Auftragsmanagement	(+)
	Strenge Auswahl der Dienstleister	(+)
	Vorabüberzeugungspflicht	(+)
	Nachkontrollen	(+)

Anlagen und Zertifikate:

- Konkrete Beschreibung der technischen und organisatorischen Maßnahmen (neurocat GmbH und Amazon Web Services EMEA SARL)
- SOC I/II/III (AWS)
- ISO/IEC 27001:2013; 270171:2015; 27018:2019; 27701:2019; 22301:2019; 90001:2015
- CSA STAR CCM v4.0

d) Procedures for periodic review, assessment and evaluation (Art. 32 (1) (d), 25 (1) GDPR)

Data protection management In the event of a personal data breach, a documented process is in place that details the steps to be taken to minimise the resulting risks. This includes, in particular, the reporting obligations and deadlines that apply, as well as the contact details and procedures required for reporting.		(+)
Incident Response Management (IRM)		(+)
Data processing control No DP without instructions from the Contracting Party	Drafting of contracts	(+)
	Formalised data management	(+)
	Rigorous selection of service providers	(+)
	Vetting duty	(+)
	Follow-up checks	(+)

Annexes and certificates:

- Specific description of technical and organisational measures (neurocat GmbH and Amazon Web Services EMEA SARL)
- SOC I/II/III (AWS)
- ISO/IEC 27001:2013; 270171:2015; 27018:2019; 27701:2019; 22301:2019; 90001:2015
- CSA STAR CCM v4.0

Konkrete Ausgestaltung der technischen und organisatorischen Maßnahmen

I. Allgemeine Informationen

In den Büroräumen des Auftragsverarbeiters selbst gibt es keine Server. Die von Amazon Web Services EMEA SARL („AWS“) betriebenen Server stehen in den Rechenzentren in Deutschland. Weitere Informationen zu den Sicherheitsprozessen der AWS-Rechenzentren finden Sie hier:

- AWS Cloud-Sicherheit
- AWS Datenschutzhinweise
- AWS Datenschutz in Deutschland
- AWS Übersicht über die Sicherheitsprozesse

II. Zutrittskontrolle

Zutrittskontrollen im Sinne dieser Anlage meint alle Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder verwendet werden, zu verwehren.

Die Büroräume des Auftragsverarbeiters befinden sich in einem Gebäudekomplex in Berlin, dessen Zugänge entweder beaufsichtigt oder verschlossen sind. Im Erdgeschoss des Gebäudes befindet sich ein Empfang, wodurch der Zutritt zum Gebäude für Unbefugte erschwert wird. Die Büroräume des Auftragsverarbeiters sind hinter einer Eingangstür, welche mit einer Klingel versehen ist. Personen, welche über keinen Transponder verfügen, werden entsprechend durch Mitarbeiter:innen hereingelassen. Alle Türen des Gebäudekomplexes verfügen über eine elektronische Schließanlage. Das Schlüsselmanagement für die Türen liegt beim Vermieter. Die von diesem ausgegebenen Transponder sind den jeweiligen Mieter:innen zugeordnet. Die Verwaltung dieser Transponder obliegt den Mieter:innen. Für die Aus- und Rückgabe der Transponder gibt es bei dem Auftragsverarbeiter ein protokolliertes Verfahren. Dieses setzt zudem voraus, dass sowohl die Ausgabe eines Transponders an einen/eine Mitarbeiter:in als auch dessen Rückgabe durch einen/eine Mitarbeiter:in unverzüglich protokolliert wird. Dieses Verfahren findet auch auf die Rückgabe sonstigen Eigentums des Auftragsverarbeiters entsprechende Anwendung. Im Falle des Verlusts eines Transponders ist der/die entsprechende Mitarbeiter:in dazu verpflichtet, diesen unverzüglich zu melden.

Concrete description of the technical and organizational measures

I. General Information

There are no servers installed in the data processor's own offices The servers operated by Amazon Web Services EMEA SARL ("AWS") are located in data centres in Germany. You can find more information on the security processes at the AWS data centre here:

- AWS Cloud Security
- AWS Privacy Policy
- Data Protection in Germany
- AWS overview of the security processes

II. Entrance Control

Access controls within the meaning of this Annex means all measures suitable for preventing unauthorised persons from gaining access to data processing systems that process or use personal data.

The offices of neurocat GmbH are located in a building complex in Berlin, the entrances to which are either monitored or locked. All the doors in the building complex are equipped with an electronic locking system. Key management for the doors is the responsibility of the lessor. The transponders issued by the lessor are assigned to the respective tenants. The responsibility for the administration of these transponders lies with the tenants. The processor has a procedure in place based on the dual control principle for the issue and return of these transponders. One of the requirements of this procedure is that both the issue and the return of a transponder to/by an employee is immediately logged. This procedure applies analogously to the return of other property held by neurocat GmbH. The loss of a transponder is to be reported immediately by the employee concerned.

Besucher:innen können die Räumlichkeiten des Auftragsverarbeiters besuchen, werden dabei aber stets durch mindestens einen/eine Mitarbeiter:in derselben begleitet.

Visitors can visit the neurocat GmbH premises, but always need to be accompanied by at least one of the company's employees.

Die Speicherung aller Daten des Auftragsverarbeiters, die im Auftrag verarbeitet werden, erfolgt aus-schließlich in AWS-Rechenzentren von AWS in Deutschland. Dabei verschlüsselt der Auftragsverarbeiter die gespeicherten Daten nach aktuellem Stand der Technik. Darüber hinaus werden folgende Maßnahmen zur Zutrittskontrolle getroffen:

All neurocat GmbH data processed on behalf of neurocat GmbH is stored exclusively at the AWS data centre in Frankfurt on Main. The following access control measures are in place here:

Das AWS-Rechenzentrum befindet sich in unscheinbaren Gebäuden, die von außen ohne weiteres nicht als solches zu erkennen sind. Zudem wurden um das Gebäude herum physische Sicherheits-barrieren (z.B. Zäune, Wände) errichtet. Diese hindern Unberechtigte sowohl am Zutritt zum Gebäude als auch bereits zum Gelände. Sowohl das Gebäude als auch die unmittelbare Umgebung werden außerdem ständig von ausgebildeten Sicherheitskräften überwacht.

The AWS data centre is located in inconspicuous buildings that are not readily recognisable as a data centre from the outside. Physical security barriers (e.g. fences, walls) are also erected around the building. These prevent unauthorised persons from entering the building and the premises. Both the building and the immediate vicinity are constantly monitored by trained security guards as well.

Zusätzlich wird der Zutritt zu den Rechenzentren durch elektronische Zugangskontrollen verwaltet und durch eine Alarmanlage gesichert, die dann einen Alarm auslöst, sofern eine Tür aufgebrochen oder aufgehalten werden sollte. Eine berechtigte Person genehmigt den Zutritt zu dem Gebäude. Nachdem Mitarbeiter:innen- oder Lieferant:innen-Datensätze deaktiviert wurden, wird diesen Personen die Zugangsberechtigung binnen 24 Stunden entzogen.

Access to the data centre is also secured by electronic access controls and an alarm system that triggers an alarm if a door is forced or held open. An authorised person authorises access to the building. After an employee or supplier record has been disabled, access authorisation is revoked for these persons within 24 hours.

Der Zugang zu sensiblen Bereichen wird außerdem mittels Videoüberwachung überwacht. Der Besuch durch Externe ist nur nach vorheriger Registrierung möglich und erfolgt ausschließlich unter Begleitung eines/einer berechtigten Mitarbeiters/ Mitarbeiterin von AWS.

Access to sensitive areas is also monitored by video surveillance. External visits are only permitted following prior registration and only take place in the company of an authorized AWS employee.

III. Zugangskontrolle

III. Admission Control

Zugangskontrolle im Sinne dieser Anlage meint Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Access control for the purposes of this Annex means measures suitable for preventing data processing systems from being used by unauthorised persons.

Die Büroräume des Auftragsverarbeiters befinden sich im zweiten und dritten Stock, sodass diese nur durch andere Bürofenster und nicht generell öffentlich einsehbar sind. Die Einsehbarkeit kann zudem manuell durch Jalousien eingeschränkt werden.

The offices of the Data Processor are located on the second and third floors, so that they can only be overlooked from other office windows and are not generally visible to the public. Visibility can also be restricted manually using blinds.

Jede/r Mitarbeiter:in verwendet zur Arbeit mit personenbezogenen Daten einen eigenen von dem Auftragsverarbeiter bereitgestellten Computer. Diese Computer sind mit Online-Profilen ausgestatten, die ein sicheres Passwort erfordern. Dieses muss bei allgemeinen administrativen Zugängen mindestens aus zwölf Zeichen und bei technischen Identifikationssysteme mindestens aus zwanzig Zeichen bestehen und in jedem Fall mindestens drei der folgenden Elemente kombinieren: Großbuchstaben, Kleinbuchstaben, Zahlen und Symbole. Die mehrfache Verwendung eines Passworts für unterschiedliche Zugänge ist untersagt. Nach jeweils drei Monaten wird jede/r Mitarbeiter:in zur Änderung des Passworts automatisch aufgefordert. Sollte sich der Stand der Technik bei der Verwendung von Passwörtern ändern, wird der Auftragsverarbeiter die Passwortanforderungen entsprechend anpassen.

Each employee uses their own computer supplied by the Data Processor for working with personal data. These computers are equipped with online profiles that require a secure password. This has to consist of at least twelve characters for general administrative access and at least twenty characters for technical identification systems and in all cases combine at least three of the following elements: upper case letters, lower case letters, numbers and special characters. Multiple use of the same password for different logins is prohibited. Each employee is automatically prompted to change their password every three months. The Data Processor will modify the password requirements accordingly if the state of the art in password use changes.

Eine Berechtigung zur Verwendung eines IT-Systems oder eines sonstigen Programms wird bei dem Auftragsverarbeiter nur dann erteilt, wenn die Berechtigung unbedingt erforderlich ist, damit der/die Mitarbeiter:in die ihm/ihr zugewiesenen Aufgaben erfüllen kann. Dabei wird, sofern möglich, die Berechtigung auf das geringstmögliche Maß beschränkt. Die erteilten Berechtigungen und gegebenenfalls ihr Entzug, werden bei der IT-Administration protokolliert. Sofern ein/e Mitarbeiter:in seinen/ihren Aufgabenbereich wechselt, werden die Berechtigungen erneut beurteilt und gegebenenfalls korrigiert. Sollte ein/e Mitarbeiter:in das Unternehmen verlassen, werden ihm/ihr die erteilten Berechtigungen durch die IT-Administration binnen 24 Stunden nach dessen Ausscheiden entzogen.

At neurocat GmbH, authorisation to use an IT system or another programme is only granted if it is absolutely necessary for the employee to be able to perform the tasks assigned to them. As far as possible, authorisation is restricted to the lowest possible level. The IT administration logs the authorisations granted and, if applicable, their withdrawal. If an employee moves to another area of responsibility, the authorisations are reassessed and corrected if necessary. If an employee leaves the company, the IT administration withdraws the authorisations granted to them within 24 hours of leaving.

Der Zugriff auf die externen IT-Systeme von AWS erfolgt ausschließlich über verschlüsselte Systeme. Die dabei verwendeten Verschlüsselungsalgorithmen und Schlüssellängen entsprechen dem Stand der Technik. Für den Zugang zu den AWS-Systemen mit produktiv genutzten Daten ist darüber hinaus eine Zwei-Faktor-Authentisierung notwendig.

Access to the external AWS IT systems takes place exclusively over encrypted systems. The encryption algorithms and key lengths used correspond to the state of the art. In addition, two-factor authentication is required to access AWS systems that contain production data.

Alle IT-Systeme, mit denen Daten im Auftrag verarbeitet werden, sind mit einer Antivirus-Software ausgestattet. Jedes Arbeitsgerät verfügt über einen passwortgesicherten Bildschirmschoner, der sich in der Regel nach fünf Minuten Inaktivität automatisch aktiviert.

All IT systems used to process data on behalf of the neurocat GmbH are equipped with anti-virus software. Each work device is equipped with a password-protected screen saver that normally activates automatically after five minutes of inactivity.

Die im Rahmen der Applikationsentwicklung verwendeten Images und Libraries werden

The images and libraries used in application development are regularly scanned for

regelmäßig einem Vulnerability Scan unterzogen. Ergebnisse mit signifikanter Relevanz werden protokolliert, im aktuellen Kontext bewertet und etwaige Folgemaßnahmen referenziert. Darüber hinaus findet eine regelmäßige Überprüfung der IT-Sicherheitsstandards statt. Die darin identifizierten Maßnahmen werden zeitnah umgesetzt.

Auch bei den AWS-Rechenzentren werden die Berechtigungen nach dem Prinzip der Minimal-berechtigungen erteilt und die erteilten Berechtigungen regelmäßig überprüft. Die Vergabe und der Ent-zug der Berechtigungen werden protokolliert. Die zu verwendenden Passwörter seitens der Mitarbeiter:innen von AWS müssen komplex sein und spätestens nach 90 Tagen wieder gewechselt werden. Für den Zugang zu Systemen mit produktiv genutzten Daten ist darüber hinaus eine Zwei-Faktor-Authentisierung notwendig.

IV. Zugriffskontrolle

Zugriffskontrollen im Sinne dieser Anlage meint alle Maßnahmen, die gewährleisten, dass die zur Benut-zung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, bei der Nutzung und nach der Speicherung nicht unbefugt verarbeitet (gelesen, kopiert, verändert oder entfernt) werden können.

Die Erteilung von Benutzungsrechten erfolgt stets nur in dem für die Aufgaben des/der entsprechenden Mitarbeiters/Mitarbeiterin geringstmöglichen Umfang. Die Erteilung und der Entzug von Berechtigungen wird protokolliert und regelmäßig überprüft. Zudem wird der Zugriff auf personenbezogene Daten (Lesen, Bearbeiten, Entfernen) protokolliert und für 30 Tage gespeichert.

Der Zugriff auf die AWS-Server erfolgt ausschließlich durch Administratoren über eine private Schlüsseldatei. Die zuständigen Mitarbeiter:innen des Auftragsverarbeiters erhalten jeweils einen eigenen Schlüssel. Mitarbeiter:innen in anderen Rollen wie Entwickler/Tester haben keinen Zugriff auf die Server, auf denen die personenbezogenen Daten des Verantwortlichen verarbeitet werden.

vulnerabilities. Significantly relevant results are recorded, assessed in the current context and any follow-up action is indicated. In addition, the IT security standards are subjected to regular review. The measures identified as part of this process are implemented without delay.

At the AWS data centre as well, authorisations are granted in accordance with the principle of minimum authorisations and the authorisations granted are regularly reviewed. Authorisations are logged when they are granted and withdrawn. The passwords to be used by AWS employees have to be complex and need to be changed again after no more than 90 days. In addition, two-factor authentication is required to access systems that contain production data.

IV. Access Control

For the purposes of this Annex, access controls means measures to ensure that persons entitled to use data processing systems have access only to the data which they have the right access, and that personal data cannot be processed (read, copied, modified or removed) without authorisation while processing, using and after saving it.

User rights are only ever granted to the minimum extent possible for the tasks performed by the respective employee. Authorisations are logged and regularly reviewed when they are granted and withdrawn. Access to personal data (read, edit, remove) is also logged and stored for 30 days.

Access to the AWS server takes place over a private key file. Each of the employees responsible at the Data Processor receive their own key. Employees in other roles such as developers/testers do not have access to the servers on which the controller's personal data is processed.

V. Trennungskontrolle

Die Trennungskontrolle im Sinne dieser Anlage beschreibt Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Systemdateien unterschiedlicher Anwendungen und die Benutzerdateien werden, sofern sie zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet. Die Trennung wird u.a. durch Verarbeitung auf dedizierten Kunden-Accounts umgesetzt, und zusätzlich durch Isolation der Kommunikation der Server-Cluster im Kunden-Account durch dedizierte Namespaces. (logische Trennung). Eine physische Trennung durch dedizierte Hosts kann auf Nachfrage bereitgestellt werden.

VI. Weitergabekontrolle

Weitergabekontrollen im Sinne dieser Anlage sind solche Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt verarbeitet (gelesen, kopiert, verändert, gelöscht) werden können. Zudem erfordern sie, dass überprüf- und feststellbar ist, an welcher Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung beabsichtigt ist.

Dadurch, dass die Erteilung von Berechtigungen sich nach dem geringstmöglichen Umfang richtet, ist die Anzahl der Mitarbeiter:innen, die Zugang zu Daten haben, die im Auftrag verarbeitet werden, auf den kleinstmöglichen Kreis beschränkt. Die Übertragung von Passwörtern und Nutzerdaten an AWS erfolgt ausschließlich über VPN-Verbindungen. Auch unabhängig von der VPN-Verbindung erfolgt die Datenübertragung in Cloud-Systeme stets verschlüsselt (nach aktuellem Stand der Technik). Sollten im Einzelfall auf Anfrage des Auftraggebers hin, an diesen durch den Auftragsverarbeiter Daten übergeben werden, so vereinbaren die Parteien im Voraus eine sichere Verschlüsselungsmethode bzw. einen sicheren Übertragungsweg.

VII. Eingabekontrolle

Eingabekontrolle im Sinne dieser Anlage meint solche Maßnahmen, die gewährleisten, dass nach-träglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten

V. Seperation Rule

The separation rule for the purposes of this Annex describes measures to ensure that data collected for different purposes can be processed separately.

The system files from different applications and the user files, if collected for different purposes, are processed separately. Among other things, separation is achieved by processing data in dedicated client accounts and by using dedicated namespaces to isolate communication between server clusters in the client account (logical separation). Physical separation using dedicated hosts can be provided on demand.

VI. Disclosure Control

For the purposes of this Annex, disclosure controls refer to those measures which ensure that personal data cannot be processed (read, copied, modified, deleted) in an unauthorised manner during electronic transfer, during their transport or while stored on data carriers. They also require the point at which a transfer of personal data by means of data transfer equipment is intended to be verifiable and ascertainable.

Since authorisations are granted to the smallest possible extent, the number of employees who have access to data processed on behalf of neurocat GmbH is limited to the smallest possible group. Passwords and user data are transferred to AWS over VPN connections only. Data transfer to cloud systems is always encrypted (using the latest technology). This takes place independent of the VPN connection. If, in individual cases, neurocat GmbH transfers data to the Contracting Party at the Contracting Party's request, the Parties agree in advance on a secure encryption method or a secure means of transfer.

VII. Input Control

Input control for the purposes of this Annex means those measures to ensure that it is possible to check and establish retroactively

in Daten-verarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Der Auftragsverarbeiter ist mittels Protokollierungs- und Auswertungssysteme in der Lage, nachträglich alle etwaigen Veränderungen an der Datenverwaltung nachzuvollziehen bzw. zu dokumentieren. Dies geschieht mit Hilfe von Auswertungssystemen, die auch die Person, die die Veränderung vorgenommen hat, erfassen.

Der Auftragsverarbeiter stellt durch eine Deletion-Engine und Orphan-Collection-Service die vollständige Löschung von Daten sicher, unter Berücksichtigung abhängiger Objekte und der notwendigen referenziellen Integrität.

Die Systemzugriffe, manuell wie automatisiert, werden vom Auftraggeber protokolliert und mindestens 30 Tage separat und ohne Löschmöglichkeit gespeichert.

VIII. Verfügbarkeitskontrolle

Unter Verfügbarkeitskontrolle im Sinne dieser Anlage sind alle Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die für den Auftraggeber verarbeiteten Daten befinden sich in den AWS-Rechenzentren in Deutschland. Der Auftragsverarbeiter hat Maßnahmen zur Sicherung und gegebenenfalls Wiederherstellung der Daten getroffen. Im Rahmen des Applikationsbetriebs werden regelmäßige Backups erstellt. Mit Hilfe dieser Backups werden regelmäßig Tests durchgeführt, die die vollständige Wiederherstellbarkeit der Applikation auf Basis der Backups gewährleisten.

Auch in den Rechenzentren von AWS wurden umfangreiche Maßnahmen zur Gewährleistung der Verfügbarkeit der Daten getroffen, wie z.B. ein auf Rauchsensoren basierendes System zur automatischen Erkennung und Bekämpfung von Bränden in den Räumen der Rechenzentren Zudem ist die Stromversorgung der Rechenzentren redundant angelegt. Daher führt auch eine mögliche Unterbrechung des Stromflusses aufgrund eines Stromausfalls nicht zu einer Unterversorgung der kritischen Bereiche der Rechenzentren mit Strom. Dies wird unter anderem über eigene Notstromaggregate gewährleistet, die im Falle eines Stromausfalls den Betrieb mit Notstrom versorgen können.

whether and by whom personal data from processing systems was entered, modified or removed.

By using logging and evaluation systems, neurocat GmbH is able to subsequently trace and document all eventual changes to the data administration. This takes place with the assistance of evaluation systems that also register the person who made the change.

The Data Processor uses a deletion engine and an orphan collection service to ensure that data is deleted in its entirety, taking into account dependent objects and the required referential integrity.

All instances of system access, both manual and automated, are logged by the Contracting Party and stored separately for at least 30 days without the possibility of deletion.

VIII. Availability Control

For the purposes of this Annex, availability control means all measures to ensure that personal data is protected from accidental loss or destruction.

All data processed for the Contracting Party is located at the AWS data centre in Frankfurt on Main, Germany. neurocat GmbH has taken measures to back up and, if necessary, restore the data. Regular backups are made while the application is in operation. These backups are used to run regular tests to ensure that the application can be fully recovered from the backups.

Extensive measures have also been taken at the AWS data centre to ensure data availability, such as a smoke detector-based system to automatically detect and fight fires in the rooms at the data centre. The power supply at the data center is also redundant. This means that even an eventual disruption in the supply of electricity caused by a blackout does not lead to an insufficient supply of electricity to the critical areas in the data centre. Among other things, this is guaranteed by the in-house emergency power generators, which can supply the operation with emergency power in the event of a blackout. AWS also carries out preventive maintenance to safeguard the continued operation of the data

AWS führt außerdem vorbeugende Wartungsmaßnahmen durch, um den fortlaufenden Betrieb der Rechenzentren zu gewährleisten.

Zusätzlich erhöhen Firewalls (Security Groups, Network Access Control Lists, Micro-Service-Firewalls) und Denial of Service Vorkehrungsmaßnahmen wie AWS Shield die Verfügbarkeit des Systems.

Die Verarbeitung, insbesondere die Speicherung, erfolgt in der AWS-Cloud mit regional ausgelegter Redundanz und trägt zur Verlässlichkeit sowie hohen Datenverfügbarkeit bei. Die Systeme sind in Infrastructure-as-Code definiert und können bei Bedarf ersetzt oder dupliziert werden.

IX. Auftragskontrolle

Auftragskontrolle im Sinne dieser Anlage ist jede Maßnahme, die gewährleistet, dass personen-bezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftrag-gebers verarbeitet werden können.
Der Auftragsverarbeiter ist bestrebt, den höchstmöglichen Schutz personenbezogener Daten zu gewährleisten. Dafür sind alle Mitarbeiter:innen zur Vertraulichkeit verpflichtet.

Alle Mitarbeiter:innen, die direkt an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, wurden im Hinblick auf den Schutz personenbezogener Daten bei deren Verarbeitung instruiert. Sollte der Auftraggeber darüberhinausgehende, ergänzende Weisungen erteilen, wird der Auftragsverarbeiter alle betroffenen Mitarbeiter:innen unverzüglich über die jeweiligen Weisungen informieren und entsprechende Handlungsanweisungen zu deren Umsetzung geben.

Um den Datenschutz kontinuierlich zu verbessern, reevaluiert der Auftragsverarbeiter zudem regelmäßig seine Verträge mit Unterauftragsverarbeiter und die getroffenen technisch-organisatorischen Maßnahmen zur Datensicherheit. Zudem werden etwaige Verbesserungsvorschläge der Mitarbeiter:innen in einem Prozess der kontinuierlichen Verbesserung des Umgangs mit diesen Daten einbezogen.

AWS ist zur Einhaltung der Datenschutzstandards nach EU-Recht verpflichtet und die Daten werden physisch ausschließlich innerhalb der EU gespeichert und nicht in Drittländer übermittelt.

centre.

In addition, firewalls (security groups, network access control lists, micro-service firewalls) and denial-of-service protection such as AWS Shield increase system availability.

Processing, especially storage, takes place in the AWS cloud with regionally configured redundancy, contributing to reliability and the high availability of data. The systems are defined in infrastructure as code and can be replaced or duplicated as required.

IX. Data processing control

For the purposes of this Annex, "data control" means any measures taken to ensure that personal data processed on behalf of neurocat GmbH can be processed strictly in accordance with the instructions of the Contracting Party. The processor strives to ensure the highest possible level of protection for personal data. All employees are obliged to maintain confidentiality for this purpose.

All employees directly involved in providing services to the Contracting Party have received instruction concerning the protection of personal data when processing such data. If the Contracting Party issues additional instructions, neurocat GmbH will immediately inform all the employees concerned of the corresponding instructions and give appropriate directions on how to implement them.

In order to constantly improve data protection, neurocat GmbH also regularly re-evaluates their agreements with subcontractors and the technical and organisational measures taken to ensure data security. In addition, any suggestions for improvement made by employees are incorporated into a process of continuous improvement in handling such data.

In addition to the General Terms and Conditions, a DPA was also concluded with AWS in accordance with the statutory provisions. In

accordance with this, AWS is obliged to comply with data protection standards under European Union law and the data is stored physically in Germany alone and is not transferred to third countries.

Anlage 3 – Liste der Unterauftragsverarbeiter

Eine Liste der vom Auftragsverarbeiter, mit Zustimmung des Auftraggebers, eingesetzten Unterauftragsverarbeiter.

Unterauftragnehmer	Anschrift/Land	Leistung
Amazon Web Services EMEA SARL (“AWS”)	38, Avenue John F. Kennedy, L-1855 Luxembourg Speicherort: Deutschland	Server Hosting, Cloud-Computing-Services und Betriebsaufgaben

Annex 3 – List of sub-processors

A list of sub-processors deployed by the Data Processor with the consent of the Contracting Party.

Subcontractor	Address/country	Service
Amazon Web Services EMEA SARL (AWS Frankfurt)	38, Avenue John F. Kennedy, L-1855 Luxembourg Storage location: Germany	Hosting and operations