parcelLab

parcelLab

Data Processing Agreement (EN-DE)

Applicable to parcelLab's Master Service Agreement

Version 5.0

May 2025

Data Processing Agreement	Auftragsverarbeitungsvertrag
This Data Processing Agreement ("**DPA**") is entered into by and between parcelLab and the Customer and governs the Processing of End-User Personal Data by parcelLab in connection with the Services provided under the Agreement as defined below. This DPA is effective as of the date of last signature ("**Effective Date**").	Dieser Auftragsverarbeitungsvertrag („**AVV**") wird von und zwischen parcelLab und dem Kunden abgeschlossen und regelt die Verarbeitung personenbezogener Endnutzerdaten durch parcelLab im Zusammenhang mit den Diensten, die im Rahmen des Vertrags erbracht werden. Dieser AVV tritt am Tag der letzten geleisteten Unterschrift in Kraft („**Datum des Inkrafttretens**").
1. DEFINITIONS Capitalised terms not defined herein shall have the meaning provided in the Agreement. Terms used, such as "**Personal Data**","**Process"/"Processing**","**Controller**", "**Processor**", and "**Data Subject**" shall have the meanings set forth in Article. 4 of the GDPR. For the purpose of this DPA: **1.1** "**Agreement**" means the agreement for parcelLab Services entered into by the Parties, of which this DPA forms part of. **1.2** "**Data Protection Legislation**" means any applicable data privacy laws and regulations, including but not limited to, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the UK GDPR as incorporated into the Data Protection Act 2018, the California Consumer Privacy Act ("**CCPA**"), and any other applicable data protection laws in the jurisdiction where Personal Data is processed under this DPA. **1.3** "**End User**" means an individual who interacts as a customer or user of the Customer's products or services. **1.4** "**End-User Personal Data**" means any personal data or information related to an End-User that is collected and Processed through the Platform. **1.5** "**Parties**" (each individually also a "**Party**") means parcelLab and the Customer. **1.6** "**Platform**" means parcelLab's proprietary shipping and communication software services web-based portal. **1.7** "**Service(s)**" means all services provided by parcelLab in connection with the Customer's use of the Platform, as specified in the Agreement.	**1. BEGRIFFSBESTIMMUNGEN** Fett geschriebene Begriffe, die hier nicht definiert sind, haben die im Vertrag festgelegte Bedeutung. Verwendete Begriffe wie „**personenbezogene Daten**", „**verarbeiten**"/„**Verarbeitung**", „**Verantwortlicher**", „**Auftragsverarbeiter**" und „**betroffene Person**"/„**Betroffener**" haben die in Art. 4 DSGVO festgelegte Bedeutung. Für die Zwecke dieses AVV gilt Folgendes: **1.1** „**Vertrag**" bezeichnet den von den Parteien abgeschlossenen Vertrag über die parcelLab-Dienste, zu dem dieser AVV gehört. **1.2** „**Datenschutzgesetzgebung**" bedeutet alle anwendbaren Datenschutzgesetze und -vorschriften, einschließlich, aber nicht beschränkt auf die Allgemeine Datenschutzverordnung (EU) 2016/679 („**DSGVO**"), die UK GDPR, wie sie in den Data Protection Act 2018 aufgenommen wurde, den California Consumer Privacy Act („**CCPA**") und alle anderen anwendbaren Datenschutzgesetze in dem Land, in dem personenbezogene Daten gemäß diesem AVV verarbeitet werden. **1.3** „**Endnutzer**" bezeichnet eine Person, die als Kunde oder Nutzer mit den Produkten oder Diensten des Kunden interagiert. **1.4** „**Personenbezogene Daten des Endnutzers**" sind alle personenbezogenen Daten oder Informationen in Bezug auf einen Endnutzer, die über die Plattform gesammelt und verarbeitet werden. **1.5** „**Parteien**" (jede für sich auch eine "**Partei**") bezeichnet parcelLab und den Kunden. **1.6** „**Plattform**" bezeichnet das proprietäre webbasierte Portal für Versand- und

	Kommunikationssoftwaredienste von parcelLab. **1.7** „**Dienst(e)**" bezeichnet alle von parcelLab in Verbindung mit der Nutzung der Plattform durch den Kunden erbrachten Dienstleistungen, wie im Vertrag festgelegt.
2. PROCESSING INSTRUCTIONS BY THE CONTROLLER **2.1 Processor and Controller.** For the purposes of this Agreement, the Customer (the "**Controller**"), is instructing parcelLab (the "**Processor**"), to engage in the rocessing of End-User Personal Data under the terms, conditions and limits detailed herein. **2.2 Scope and Purpose of Processing.** The Processor shall Process End-User Personal Data solely as required to deliver the Services described in the Agreement, in accordance with the Controller's documented instructions. This includes the analysis and processing of user, recipient, usage, order, and shipment information to: (i) keep End Users informed of delivery status; (ii) facilitate returns and logistical processing of shipments; (iii) enable personalised or targeted communications and campaigns to End Users; (iv) assess the performance of logistics service providers through analysis of data transmitted by the Controller and logistics service providers; (v) provide a transparent presentation of shipment events, such as location and time-based stamps/status messages; and (vi) support the Controller in enhancing End User communications through order and shipment information analysis. **2.3 Categories of Data Subjects and Types of Personal Data.** The categories and types of End-User Personal Data Processed under this DPA shall include: • **Data Subjects:** End Users. • **Personal Data:** names; salutations; addresses; contact details (e.g. email, phone numbers and channel identifiers); order and shipment information (e.g. order number, product	**2. VERARBEITUNGSANWEISUNGEN DURCH DEN VERANTWORTLICHEN** **2.1 Auftragsverarbeiter und Verantwortlicher.** Für die Zwecke dieses Vertrags beauftragt der Kunde (der „**Verantwortliche**") parcelLab (den „**Auftragsverarbeiter**") mit der Verarbeitung der personenbezogenen Daten des Endnutzers unter den hier aufgeführten Bedingungen und Einschränkungen. **2.2 Umfang und Zweck der Verarbeitung.** Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Endnutzers ausschließlich soweit es für die Erbringung der im Vertrag beschriebenen Dienste erforderlich ist, und zwar in Übereinstimmung mit den dokumentierten Anweisungen des Verantwortlichen. Dies beinhaltet die Analyse und Verarbeitung von Benutzer-, Empfänger-, Nutzungs-, Bestell- und Versandinformationen, um: (i) die Endnutzer über den Lieferstatus zu informieren; (ii) Retouren und die logistische Abwicklung von Sendungen zu erleichtern; (iii) personalisierte oder gezielte Mitteilungen und Kampagnen an Endnutzer zu ermöglichen; (iv) die Leistung von Logistikdienstleistern durch Analyse der von der Verantwortlichen und den Logistikdienstleistern übermittelten Daten zu bewerten; (v) eine transparente Darstellung von Sendungsereignissen, wie z. B. orts- und zeitbezogene Aufzeichnungen/Statusmeldungen zu ermöglichen; und (vi) den Verantwortlichen bei der Verbesserung der Kommunikation mit den Endnutzern durch die Analyse von Bestell- und Sendungsinformationen zu unterstützen. **2.3 Kategorien betroffener Personen und Arten personenbezogener Daten.** Zu den Kategorien und Arten personenbezogener Daten der

number, products purchased, prices, payment method, shipment number and carrier details); tracking updates from the carrier (e.g. signatures or images and names of delivery contacts provided by the Controller); and any other Personal Data that the End-User may provide, or that the Controller may instruct the Processor to Process (e.g. marketing preferences). **2.4 Duration of the DPA.** The terms and obligations of this DPA shall continue for the duration of the Agreement, or as long as Processor Processes End User Personal Data under the Agreement. Upon termination of the Agreement or earlier upon the Controller's request, Processor shall delete or return all End-User Personal Data in its possession in accordance with Section 11 below, unless otherwise required by law. **2.5 Data retention Period.** Unless otherwise requested in writing by the Controller, Processor shall delete all End-User Personal Data in its possession that is used for Processing automatically and on a rolling basis after ninety (90) days.	Endnutzer, die im Rahmen dieses AVV verarbeitet werden, gehören: • **betroffene Personen:** Endnutzer • **personenbezogene Daten:** Name, Anrede, Adresse, Kontaktdaten (z. B. E-Mail-Adresse, Telefonnummer und Kanalidentifikatoren), Bestell- und Versandinformationen (z. B. Bestellnummer, Produktnummer, gekaufte Produkte, Preise, Zahlungsmethode, Versandnummer und Angaben zum Carrier), Aktualisierungen der Sendungsverfolgung durch den Carrier(z. B. Unterschriften oder Bilder und Namen der vom Verantwortlichen bereitgestellten Zustellkontakte) sowie sonstige personenbezogene Daten, die der Endnutzer zur Verfügung stellt oder die der Verantwortliche dem Auftragsverarbeiter zur Verarbeitung anweist (z. B. Marketingpräferenzen). **2.4 Dauer des AVV.** Die Bedingungen und Verpflichtungen dieses AVV gelten für die Dauer des Vertrags oder so lange, wie der Auftragsverarbeiter personenbezogene Daten des Endnutzers im Rahmen des Vertrags verarbeitet. Bei Beendigung des Vertrags oder auf Verlangen des Verantwortlichen zu einem früheren Zeitpunkt hat der Auftragsverarbeiter alle in seinem Besitz befindlichen personenbezogenen Daten der Endnutzer gemäß Abschnitt 11 zu löschen oder zurückzugeben, sofern nicht lich anders vorgeschrieben. **2.5 Dauer der Datenspeicherung.** Sofern der Verantwortliche nichts anderes schriftlich verlangt, löscht der Auftragsverarbeiter alle in seinem Besitz befindlichen personenbezogenen Daten der Endnutzer, die für die Verarbeitung verwendet wurden, automatisch und fortlaufend nach neunzig (90) Tagen.
3. PROCESSOR OBLIGATIONS **3.1 Follow Controller's Instructions**. Processor shall Process End-User Personal Data only in accordance with the documented instructions provided by the Controller, including the purposes, scope and limits set forth in this DPA to fulfil the terms of the Agreement. If Processor believes that an instruction violates applicable Data Protection Legislation, it shall promptly notify the Controller.	**3. VERPFLICHTUNGEN DES AUFTRAGSVERARBEITERS** **3.1 Befolgung der Anweisungen des Verantwortlichen.** Der Auftragsverarbeiter darf personenbezogene Daten des Endnutzers nur gemäß den dokumentierten Anweisungen des Verantwortlichen verarbeiten, einschließlich der Zwecke, des Umfangs und der Grenzen, die in diesem AVV zur Erfüllung der Bedingungen des Vertrags festgelegt sind. Ist der Auftragsverarbeiter der Ansicht, dass eine

3.2 Assistance with Data Subject Rights. The Processor shall, considering the nature of the Processing, assist the Controller in fulfilling its obligations to respond to Data Subject requests under applicable Data Protection Legislation. Such assistance shall include implementing appropriate technical and organisational measures (**TOMs**) to address requests for access, rectification, erasure, restriction, portability, and objection, or any other right afforded to Data Subjects under applicable Data Protection Legislation. If a Data Subject submits a request directly to the Processor regarding their data, the Processor shall forward such request to the Controller without undue delay. The Processor shall not take any action to modify, delete, or restrict any End-User Personal Data, or otherwise respond to the Data Subject's request, unless explicitly instructed in writing by the Controller.	Anweisung gegen geltendes Datenschutzgesetzgebung verstößt, hat er den Verantwortlichen unverzüglich zu benachrichtigen. **3.2 Unterstützung bei der Wahrnehmung der Rechte der betroffenen Person.** Der Auftragsverarbeiter unterstützt den Verantwortlichen in Bezug auf die Verarbeitung bei der Erfüllung seiner Verpflichtungen zur Beantwortung von Anfragen Betroffener gemäß der geltenden Datenschutzgesetzgebung. Diese Unterstützung umfasst die Umsetzung geeigneter technischer und organisatorischer Maßnahmen (**TOM**), um Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit und Widerspruch oder anderen Rechten nachzukommen, die den betroffenen Personen nach der geltenden Datenschutzgesetzgebung zustehen. Stellt eine betroffene Person einen Antrag bezüglich ihrer Daten direkt an den Auftragsverarbeiter, so leitet dieser den Antrag ohne unangemessene Verzögerung an den Verantwortlichen weiter. Der Auftragsverarbeiter ergreift keine Maßnahmen zur Änderung, Löschung oder Einschränkung personenbezogener Daten des Endnutzers oder zur sonstigen Beantwortung des Antrags der betroffenen Person, es sei denn, der Verantwortliche erteilt ausdrücklich eine schriftliche Anweisung.
3.3 Assistance with Data Protection Impact Assessments (DPIAs). The Processor shall provide reasonable assistance to the Controller in carrying out Data Protection Impact Assessments taking into account the nature of Processing and the information available to the Processor.	**3.3 Unterstützung bei Datenschutz-Folgenabschätzungen (DSFA).** Der Auftragsverarbeiter unterstützt den Verantwortlichen in angemessener Weise bei der Durchführung von Datenschutz-Folgenabschätzungen unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.
3.4 Consultation with Supervisory Authorities. The Processor shall assist the Controller in any required consultations with supervisory authorities, including by providing relevant details about Processing activities, responding to inquiries, and addressing complaints or investigations. The Controller shall promptly notify the Processor of any breaches, complaints, or investigations and provide the necessary support and information to facilitate the Processor's obligations under the applicable Data Protection Legislation.	**3.4 Konsultation mit den Aufsichtsbehörden.** Der Auftragsverarbeiter unterstützt den Verantwortlichen bei allen erforderlichen Konsultationen mit den Aufsichtsbehörden, indem er unter anderem sachdienliche Angaben zu den Verarbeitungstätigkeiten macht, auf Anfragen antwortet und sich mit Beschwerden oder Untersuchungen befasst. Der Verantwortliche unterrichtet den Auftragsverarbeiter unverzüglich über Verstöße, Beschwerden oder Untersuchungen und stellt ihm die erforderliche Unterstützung
3.5 Notification of Data Breaches. In the event of any unauthorised access, disclosure, alteration, or loss of End-User Personal Data due to a breach of security ("**Data Breach**"), the Processor shall notify the Controller without undue delay, and in any event no later than within seventy-two (72) hours after becoming aware of the Data Breach. Such notification shall include a detailed	

report containing, to the extent reasonably available: the nature of the breach, the categories and approximate volume of the data involved, and actions taken to mitigate further risk. The Processor shall assist the Controller in meeting any legal obligations to report Data Breaches to supervisory authorities and, where applicable, to affected Data Subjects, if the Controller deems such notification necessary. **3.6 Confidentiality and Access Controls.** Processor shall ensure that only authorised employees trained in data protection and bound by confidentiality agreements have access to End-User Personal Data. **3.7 Internal Monitoring and Compliance.** Processor shall monitor internal processes and TOMs at least annually, or more frequently as necessary, to ensure compliance with Data Protection Laws. Processor shall promptly take corrective measures to address any risks or gaps identified, with particular attention to protecting the rights and freedoms of data subjects.	und Informationen zur Verfügung, um die Verpflichtungen des Auftragsverarbeiters gemäß den geltenden Datenschutzvorschriften zu erfüllen. **3.5 Benachrichtigung über Datenschutzverletzungen.** Im Falle eines unbefugten Zugriffs, einer unbefugten Offenlegung, einer unbefugten Änderung oder eines unbefugten Verlusts von personenbezogenen Daten des Endnutzers aufgrund einer Sicherheitsverletzung („**Datenschutzverletzung**“) benachrichtigt der Auftragsverarbeiter den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von zweiundsiebzig (72) Stunden nach Bekanntwerden der Datenschutzverletzung. Diese Benachrichtigung umfasst einen detaillierten Bericht, der, soweit dies vernünftigerweise möglich ist, Folgendes enthält: die Art der Verletzung, die Kategorien und den ungefähren Umfang der betroffenen Daten sowie die Maßnahmen, die zur Behebung weiterer Risiken getroffen wurden. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung etwaiger rechtlicher Verpflichtungen zur Meldung von Datenschutzverletzungen an Aufsichtsbehörden und gegebenenfalls an betroffene Personen, wenn der Verantwortliche eine solche Meldung für erforderlich hält. **3.6 Vertraulichkeit und Zugangskontrollen.** Der Auftragsverarbeiter stellt sicher, dass nur befugte, im Datenschutz geschulte und zur Vertraulichkeit verpflichtete Mitarbeiter Zugang zu den personenbezogenen Daten der Endnutzer haben. **3.7 Interne Überwachung und Einhaltung.** Der Auftragsverarbeiter überwacht die internen Prozesse und TOM mindestens einmal jährlich bzw. bei Bedarf häufiger, um die Einhaltung der Datenschutzgesetzgebung zu gewährleisten. Der Auftragsverarbeiter ergreift unverzüglich Abhilfemaßnahmen, um festgestellte Risiken oder Lücken zu beseitigen, wobei er besonders auf den Schutz der Rechte und Freiheiten der betroffenen Personen achtet.
4. CONTROLLER RIGHTS AND OBLIGATIONS **4.1 Compliance.** The Controller warrants that it has complied with all applicable Data Protection Legislation and confirms that: i) it has secured all necessary permissions,	**4. RECHTE UND PFLICHTEN DES VERANTWORTLICHEN** **4.1 Compliance.** Der Verantwortliche gewährleistet, dass er die geltende Datenschutzgesetzgebung einhält und

consents, and disclosures to permit Processor to lawfully process End-User Personal Data provided by or on behalf of the Controller in accordance with this DPA and any applicable laws; ii) End-User Personal Data has been collected lawfully, fairly, and transparently; iii) the End-User Personal Data provided to the Processor is accurate, complete, and up-to-date; and iv) Data Subjects have been informed of the Processing activities and the involvement of third-party processors, where required.

4.2 Controller Responsibility for Costs. The Controller agrees to bear costs arising from non-standard or additional instructions beyond those agreed in this DPA or the Agreement, compliance with Data Subject rights requests that require Processor to perform actions outside the agreed scope, and rectifying errors caused by inaccurate or incomplete End-User Personal Data.

4.3 Documentation and Instructions. In addition to the instructions set out in Section 2 of this DPA, the Controller may provide Processor with additional or rectifying instructions. Such instruction shall be clear and documented.

4.4 Additional Instructions. The Controller has the right to issue additional instructions regarding the Processing of End-User Personal Data by contacting the Processor at support@parcellab.com. If any instruction conflict with applicable Data Protection Legislation, the Processor may notify the Controller and suspend the affected Processing until instructions are confirmed or revised.

bestätigt, dass: i) er alle erforderlichen Genehmigungen, Einwilligungen und Offenlegungen eingeholt hat, um dem Auftragsverarbeiter die rechtmäßige Verarbeitung der von dem Verantwortlichen oder in seinem Namen bereitgestellten personenbezogenen Daten der Endnutzer gemäß diesem AVV und den geltenden Gesetzen zu ermöglichen; ii) die personenbezogenen Daten der Endnutzer auf rechtmäßige, faire und transparente Weise erhoben wurden; iii) die dem Auftragsverarbeiter zur Verfügung gestellten personenbezogenen Daten der Endnutzer richtig, vollständig und aktuell sind; und iv) die betroffenen Personen über die Verarbeitungstätigkeiten und die Einbeziehung von Drittverarbeitern, sofern erforderlich, informiert wurden.

4.2 Verantwortung des Verantwortlichen für Kosten. Der Verantwortliche erklärt sich bereit, die Kosten zu tragen, die sich aus nicht standardmäßigen oder zusätzlichen Anweisungen ergeben, die über die in diesem AVV oder im Vertrag vereinbarten Anweisungen hinausgehen, sowie die Kosten für die Erfüllung der Rechte der betroffenen Personen, die von dem Auftragsverarbeiter verlangen, Maßnahmen außerhalb des vereinbarten Umfangs durchzuführen, und die Kosten für die Berichtigung von Fehlern, die durch ungenaue oder unvollständige personenbezogene Daten der Endnutzer verursacht werden.

4.3 Dokumentation und Anweisungen. Zusätzlich zu den in Abschnitt 2 dieses AVV aufgeführten Anweisungen kann der Verantwortliche dem Auftragsverarbeiter zusätzliche oder berichtigende Anweisungen erteilen. Solche Anweisungen müssen eindeutig und dokumentiert sein.

4.4 Zusätzliche Anweisungen. Der Verantwortliche hat das Recht, zusätzliche Anweisungen bezüglich der Verarbeitung personenbezogener Daten der Endnutzer zu erteilen, indem er den Auftragsverarbeiter unter support@parcellab.com kontaktiert. Sollte eine Anweisung im Widerspruch zur geltenden Datenschutzgesetzgebung stehen, kann der

	Auftragsverarbeiter den Verantwortlichen benachrichtigen und die betroffene Verarbeitung aussetzen, bis die Anweisungen bestätigt oder überarbeitet sind.
5. SUB-PROCESSORS **5.1 Authorisation and Notification of Sub-processors.** The Controller authorises Processor to engage Sub-processors as necessary to fulfill Processor's obligations under the Agreement, subject to this DPA. As of the Effective Date of this DPA, the Sub-processors listed at https://parcellab.com/sub-processors/ are deemed authorised by the Controller. Processor shall notify the Controller at least ten (10) business days in advance of engaging any new Sub-processor. If the Controller does not object within ten (10) business days, the Processor may proceed with the appointment. **5.2 Sub-processor Due Diligence.** Processor shall select and engage Sub-processors with due diligence to ensure they meet data protection and security standards required under this DPA. Processor shall ensure that all Sub-processors enter into contractual obligations that reflect the requirements of this DPA and applicable Data Protection Legislation.	**5. UNTERAUFTRAGSVERARBEITER** **5.1 Genehmigung von und Benachrichtigung über Unterauftragsverarbeiter.** Der Verantwortliche ermächtigt den Auftragsverarbeiter, Unterauftragsverarbeiter zu beauftragen, soweit dies zur Erfüllung der Verpflichtungen des Auftragsverarbeiters im Rahmen des Vertrags gemäß diesem AVV erforderlich ist. Ab dem Datum des Inkrafttretens dieses AVV gelten die unter https://parcellab.com/sub-processors/ aufgeführten Unterauftragsverarbeiter als vom Verantwortlichen genehmigt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen mindestens zehn (10) Werktage im Voraus über die Beauftragung eines neuen Unterauftragsverarbeiters. Erhebt der Verantwortliche nicht innerhalb von zehn (10) Werktagen Einspruch, kann der Auftragsverarbeiter mit der Beauftragung fortfahren. **5.2 Überprüfung des Unterauftragsverarbeiters.** Der Auftragsverarbeiter hat Unterauftragsverarbeiter mit der gebotenen Sorgfalt auszuwählen und zu beauftragen, um sicherzustellen, dass sie die gemäß dieses AVV erforderlichen Datenschutz- und Sicherheitsstandards erfüllen. Der Auftragsverarbeiter stellt sicher, dass alle Unterauftragsverarbeiter vertragliche Verpflichtungen eingehen, die den Anforderungen dieses AVV und der geltenden Datenschutzgesetzgebung entsprechen.
6. SECURITY OF PROCESSING **6.1 Technical and Organisational Measures (TOMs).** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, the Processor shall implement and maintain appropriate TOMs to ensure a level of security	**6. SICHERHEIT DER VERARBEITUNG** **6.1 Technische und organisatorische Maßnahmen (TOM).** Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen setzt der Auftragsverarbeiter geeignete TOM ein und

appropriate to the risk, as outlined in Appendix 1 of this DPA. **6.2 Continual Improvement of Security.** Processor shall update and improve TOMs as necessary in line with technological advances, while ensuring that such updates do not reduce the security level. All significant changes shall be documented.	erhält sie aufrecht, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, wie in Anhang 1 dieses AVV dargelegt. **6.2 Kontinuierliche Verbesserung der Sicherheit.** Der Auftragsverarbeiter aktualisiert und verbessert die TOM bei Bedarf entsprechend dem technologischen Fortschritt, wobei er sicherstellt, dass diese Aktualisierungen das Sicherheitsniveau nicht verringern. Alle wesentlichen Änderungen sind zu dokumentieren.
7. CONTROLLER AUDITS AND VERIFICATION RIGHTS **7.1 Audit Rights of Controller.** The Controller shall have the right to conduct audits or appoint auditors to assess Processor's compliance with this DPA. Such audits shall be conducted during Processor's normal business hours and in a manner that does not unreasonably disrupt Processor's normal business operations. Processor shall make available documentation demonstrating compliance, provided the Controller gives reasonable notice of minimum fourteen (14) days and complies with mutually agreed audit limits. Processor reserves the right to charge a reasonable fee for audits exceeding routine compliance requirements. **7.2 Compliance Evidence and Certification.** Processor shall demonstrate compliance with this DPA and applicable Data Protection Legislation through certifications such as SOC 2 and HIPPA, and relevant; audit reports. Evidence shall be provided upon the Controller's reasonable request, in line with the agreed audit scope.	**7. PRÜFUNGS- UND NACHWEISRECHTE DES VERANTWORTLICHEN** **7.1 Prüfungsrechte des Verantwortlichen.** Der Verantwortliche hat das Recht, Prüfungen durchzuführen oder Prüfer zu bestellen, um die Einhaltung dieses AVV durch den Auftragsverarbeiter zu bewerten. Solche Prüfungen sind während der normalen Geschäftszeiten des Auftragsverarbeiters und in einer Weise durchzuführen, die den normalen Geschäftsbetrieb des Auftragsverarbeiters nicht unangemessen stört. Der Auftragsverarbeiter stellt Unterlagen zur Verfügung, die die Einhaltung der Bestimmungen belegen, sofern der Verantwortliche dies mit einer angemessenen Frist von mindestens vierzehn (14) Tagen ankündigt und die einvernehmlich vereinbarten Prüfungsfristen einhält. Der Auftragsverarbeiter behält sich das Recht vor, für Prüfungen, die über die routinemäßigen Anforderungen hinausgehen, eine angemessene Gebühr zu erheben. **7.2 Nachweis der Einhaltung und Zertifizierung.** Der Auftragsverarbeiter weist die Einhaltung dieses AVV und der geltenden Datenschutzgesetzgebung durch Zertifizierungen wie SOC 2 und HIPPA sowie durch einschlägige Prüfberichte nach. Die Nachweise sind auf angemessenes Verlangen des Verantwortlichen im Einklang mit dem vereinbarten Prüfungsumfang vorzulegen.
8. INTERNATIONAL TRANSFERS **8.1 Authorisation for International Transfers.** The Controller does not authorise the transfer of End-User Personal Data to countries outside the EU/EEA unless required under the Agreement or expressly agreed in writing by the Controller.	**8. INTERNATIONALE DATENÜBERMITTLUNGEN** **8.1 Genehmigung für internationale Übermittlungen.** Der Verantwortliche genehmigt die Übermittlung personenbezogener Daten von Endnutzern in Länder außerhalb der EU/des EWR nur, wenn dies im Rahmen des Vertrags erforderlich ist

8.2 **Data Transfer Mechanisms.** The Processor shall ensure that any transfer of End-User Personal Data to a location outside the EU/EEA is conducted in compliance with a valid data transfer mechanism as recognised by applicable Data Protection Legislation	oder der Verantwortliche ausdrücklich schriftlich zustimmt.
8.3 **Intra-Group Transfers.** Transfers of any End-User Personal Data between entities within the Processor's corporate group are hereby authorised by the Controller, provided that such transfers shall be governed by an intra-company processing agreement that ensures compliance with applicable Data Protection Legislation. For any cross-border transfers, the Processor shall ensure that such transfers are done under a valid data transfer mechanism.	**8.2** **Datenübertragungsmechanismen.** Der Auftragsverarbeiter stellt sicher, dass jede Übermittlung von personenbezogenen Daten des Endnutzers an einen Ort außerhalb der EU/des EWR in Übereinstimmung mit einem gültigen Datenübermittlungsmechanismus erfolgt, der von der geltenden Datenschutzgesetzgebung anerkannt ist.
8.4 **Assessment of Data Transfer Risks**. Prior to any transfer of End-User Personal Data to a location outside the EU/EEA, the Processor shall conduct a Transfer Impact Assessment (TIA) to evaluate the legal framework of the destination country, including the availability of enforceable rights and effective legal remedies for data subjects. The findings of this assessment shall inform the implementation of any supplementary measures required to ensure compliance with applicable Data Protection Legislation.	**8.3** **Gruppeninterne Übertragungen.** Die Übermittlung von personenbezogenen Daten des Endnutzers zwischen Unternehmen innerhalb der Unternehmensgruppe des Auftragsverarbeiters wird hiermit von dem Verantwortlichen genehmigt, vorausgesetzt, dass solche Übermittlungen durch einen unternehmensinternen Verarbeitungsvertrag geregelt werden, der die Einhaltung der geltenden Datenschutzgesetzgebung gewährleistet. Bei grenzüberschreitenden Übermittlungen stellt der Auftragsverarbeiter sicher, dass solche Übermittlungen im Rahmen eines gültigen Datenübermittlungsverfahrens erfolgen.
	8.4 **Bewertung der Risiken bei der Datenübermittlung.** Vor jeder Übermittlung personenbezogener Daten von Endnutzern an einen Ort außerhalb der EU/des EWR führt der Auftragsverarbeiter eine Datenschutz-Folgenabschätzung (DSFA) durch, um den rechtlichen Rahmen des Ziellandes zu bewerten, einschließlich der Verfügbarkeit durchsetzbarer Rechte und wirksamer Rechtsbehelfe für die betroffenen Personen. Die Ergebnisse dieser Bewertung dienen als Grundlage für die Durchführung zusätzlicher Maßnahmen, die erforderlich sind, um die Einhaltung der geltenden Datenschutzvorschriften zu gewährleisten.
9. DELETION AND RETURN OF PERSONAL DATA	**9. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN**
9.1 **Data Return or Deletion after Termination.** Upon termination of the Agreement or the cessation of Processing End-User Personal Data, Processor shall, within thirty (30) days of receiving the Controller's instructions, either return all End-User Personal Data to the Controller or securely delete it, including any backup copies, in a manner compliant with applicable Data Protection Legislation. Processor shall, upon the Controller's	**9.1** **Rückgabe oder Löschung von Daten nach Beendigung.** Nach Beendigung des Vertrags oder der Einstellung der Verarbeitung von personenbezogenen Daten von Endnutzern muss der Auftragsverarbeiter innerhalb von dreißig (30) Tagen nach Erhalt der Anweisungen des Verantwortlichen entweder alle personenbezogenen Daten der Endnutzer an den Verantwortlichen zurückgeben oder sie,

request, provide a written certification confirming the completion of the data deletion process. **9.2 Retention of Compliance Documentation.** Documentation required to demonstrate compliance with this DPA may be retained by Processor for legally required periods and may be transferred to the Controller at the end of the Agreement to relieve Processor of further retention obligations.	einschließlich aller Sicherungskopien, in einer Weise sicher löschen, die mit der geltenden Datenschutzgesetzgebung vereinbar ist. Der Auftragsverarbeiter muss auf Verlangen des Verantwortlichen eine schriftliche Bescheinigung über den Abschluss des Datenlöschungsverfahrens vorlegen. **9.2 Aufbewahrung der Compliance-Dokumentation.** Die Dokumentation, die zum Nachweis der Einhaltung dieses AVV erforderlich ist, kann vom Auftragsverarbeiter für die gesetzlich vorgeschriebenen Zeiträume aufbewahrt werden und bei Beendigung des Vertrags an den Verantwortlichen übertragen werden, um den Auftragsverarbeiter von weiteren Aufbewahrungspflichten zu entbinden.
10. DATA PROTECTION OFFICER Processor has appointed an external Data Protection Officer (DPO) who can be reached at dataprotection@parcellab.com	**10. DATENSCHUTZBEAUFTRAGTER** Der Auftragsverarbeiter hat einen externen Datenschutzbeauftragten (DSB) bestellt, der unter dataprotection@parcellab.com erreichbar ist.

Appendix 1 **Technical and Organisational Measures (TOMs)**	**Anhang 1** **Technische und organisatorische Maßnahmen (TOM)**
parcelLab undertakes to implement the following technical and organisational measures in accordance with Article 28(3)(2)(c) and Article 32 of the GDPR.	parcelLab verpflichtet sich, die folgenden technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c und Art. 32 DSGVO zu ergreifen.
1. Pseudonymisation & Encryption All End-User Personal Data processed by parcelLab is encrypted both at rest and in transit using state-of-the-art encryption protocols to safeguard data integrity and confidentiality. While End-User Personal Data is not pseudonymized during the standard retention period of 90 days, the retention period can be adjusted (extended or reduced) based on Customer requirements, ensuring flexibility and adherence to specific data handling needs.	**1. Pseudonymisierung & Verschlüsselung** Alle personenbezogenen Daten der Endnutzer, die von parcelLab verarbeitet werden, werden sowohl bei der Speicherung als auch während der Übertragung mit modernsten Verschlüsselungsprotokollen verschlüsselt, um die Integrität und Vertraulichkeit der Daten zu gewährleisten. Personenbezogene Daten von Endnutzern werden während der Standard-Aufbewahrungsfrist von 90 Tagen nicht pseudonymisiert. Die Aufbewahrungsfrist kann je nach Kundenwunsch angepasst (verlängert oder verkürzt) werden, um die Flexibilität sowie die Einhaltung spezifischer Anforderungen an die Datenverarbeitung zu gewährleisten.
2. Data Security and Confidentiality **2.1 Physical Access Control.** To prevent unauthorised access to data processing equipment, parcelLab implements the following measures: **2.1.1 Data Center Security.** Data is processed exclusively in data centers operated by Amazon Web Services (AWS), Google Cloud, and Microsoft Azure (together the "**Data Centers**"), ensuring robust physical access security. All network segments outside the perimeters of these Data Center providers are considered insecure (public) in the parcelLab production network design. Details of the Data Center's measures can be accessed via: i. **AWS:** https://aws.amazon.com/compliance/data-center/data-centers/	**2. Datensicherheit und Vertraulichkeit** **2.1 Physische Zugangskontrolle.** parcelLab ergreift folgende Maßnahmen um die IT-Infrastruktur vor unbefugtem Zugriff zu schützen: **2.1.1 Sicherheit im Rechenzentrum.** Die Daten werden ausschließlich in Rechenzentren verarbeitet, die von Amazon Web Services (AWS), Google Cloud und Microsoft Azure (zusammen die "**Rechenzentren") betrieben werden, um** eine robuste physische Zugriffssicherheit zu gewährleisten. Alle Netzwerksegmente außerhalb dieser Data Center Provider gelten im parcelLab Produktionsnetzwerkdesign als unsicher (öffentlich). Details zu den Maßnahmen des Rechenzentrums finden Sie unter:

ii. **Google Cloud:** https://www.google.com/about/datacenters/data-security/

iii. **Microsoft Azure:** https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-physical-access-security

2.1.2 **Office and Device Security.** No platform data is processed or stored in parcelLab offices or private data centers, and employee devices are secured with disk encryption and controlled by an MDM application which enforces endpoint security and offers remote wipe capabilities.

2.1.3 **Monitoring.** Platform components are safeguarded against unauthorised access and tampering using intrusion detection software.

2.1.4 **Certifications.** Continuous certification of infrastructure under SOC2 and HIPAA standards, with proof available upon request.

2.2 Logical Access Control. To prevent unauthorised access to data and information systems, parcelLab implements the following measures:

2.2.1 **Authentication and Authorisation.** parcelLab operates a dedicated authentication and authorisation component. Upon successful authentication, users are granted access tokens based on their assigned groups and roles. The component implements multi-factor authentication (MFA) for all parcelLab administrative staff. Single sign-on (SSO) authentication with MFA is available as an optional feature to all parcelLab Customers.

2.2.2 **Password Policy.** parcelLab enforces a strong password policy for all Customer user accounts to ensure secure access.

2.2.3 **Single Sign-On (SSO).** parcelLab supports and recommends SSO authentication for enhanced security and ease of use. Internal systems rely

i. **AWS:** https://aws.amazon.com/compliance/data-center/data-centers/

ii. **Google Cloud:** https://www.google.com/about/datacenters/data-security/

iii. **Microsoft Azure:** https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-physical-access-security

2.1.2 **Büro- und Gerätesicherheit.** Es werden keine Plattformdaten in parcelLab-Büros oder privaten Rechenzentren verarbeitet oder gespeichert,. Die Geräte der Mitarbeiter sind mit Festplattenverschlüsselung gesichert und werden von einer MDM-Anwendung gesteuert, die die Sicherheit dieser Endpunkte forciert und Remote-Löschfunktionen bietet.

2.1.3 **Überwachung.** Die Plattformkomponenten werden mit Hilfe einer Intrusion-Detection-Software vor unbefugtem Zugriff und Manipulation geschützt.

2.1.4 **Bescheinigungen.** Kontinuierliche Zertifizierung der Infrastruktur nach SOC2- und HIPAA-Standards, Nachweise sind auf Anfrage erhältlich.

2.2 Logische Zugriffskontrolle. Um unbefugte Zugriffe auf Daten- und Informationssysteme zu verhindern, ergreift parcelLab folgende Maßnahmen:

2.2.1 **Authentifizierung und Autorisierung.** parcelLab betreibt eine dedizierte Authentifizierungs- und Autorisierungskomponente. Nach erfolgreicher Authentifizierung werden

on SSO authentication, except for access to AWS Cloud Console. Access to AWS is governed by dedicated user accounts, which are automatically provisioned with MFA authentication for added security.	Benutzern Zugriffstoken basierend auf den ihnen zugewiesenen Gruppen und Rollen gewährt. Die Komponente implementiert eine Multi-Faktor-Authentifizierung (MFA) für alle administrativen Mitarbeiter von parcelLab. Die Single Sign-On (SSO)-Authentifizierung mit MFA steht allen parcelLab-Kunden als optionale Funktion zur Verfügung.
2.2.4 Authentication Process for System Access. i. **Internal Support Tools.** Access to internal support tools controlled via SSO and Access Control Lists (ACL), ensuring that only authorised users can gain access. ii. **Production System Infrastructure:** a. **VPN Access.** Production systems operate within a secure Virtual Private Network (VPN) hosted in AWS Virtual Private Clouds (VPC). Access to the VPN is restricted to authorised users who have specific permissions for designated SSH gateways. Certificates provisioned on per-user basis, are required for VPN access and are automatically managed through our infrastructure-as-code platform during onboarding and offboarding. b. **Permissions and Policies.** Permissions and access within VPN are governed by strict policies and user-specific controls. These ensure that only users with appropriate roles can access critical resources. c. **Database Security**. Databases within the VPNs employ encryption at rest and are protected with strong passwords. Our infrastructure-as-code approach enables secure management and rotation of database passwords, allowing swift action in response to security incidents.	**2.2.2 Passwort-Richtlinie.** parcelLab setzt eine strenge Passwortrichtlinie für alle Benutzerkonten des Kunden durch, um einen sicheren Zugriff zu gewährleisten. **2.2.3 Einmaliges Anmelden (Single Sign-On, SSO).** parcelLab unterstützt und empfiehlt die SSO-Authentifizierung für mehr Sicherheit und Benutzerfreundlichkeit. Interne Systeme sind auf die SSO-Authentifizierung angewiesen, mit Ausnahme des Zugriffs auf die AWS Cloud Console. Der Zugriff auf AWS wird durch dedizierte Benutzerkonten geregelt, die automatisch mit MFA-Authentifizierung bereitgestellt werden, um die Sicherheit zu erhöhen. **2.2.4 Authentifizierungsprozess für den Systemzugriff.** i. **Interne Support-Tools.** Der Zugriff auf interne Suuport-Tools erfolgt über SSO und Access Control Lists (ACL) und ist nur für autorisierte Benutzer möglich. ii. **Infrastruktur des Produktionssystems:** a. **VPN-Zugang.** Produktionssysteme werden in einem sicheren Virtual Private Network (VPN) betrieben, das in AWS Virtual Private Clouds (VPC) gehostet wird. Der

d. **Provisioning and Deprovisioning**. parcelLab follows a formal process for provisioning and deprovisioning user accounts. Access permissions are managed through group memberships, unique user IDs, strong passwords, and MFA are enforced to maintain secure access. e. **Password-Based Authentication.** For applications, that do not support SSO, parcelLab employs industry-standard password management systems supporting fine-grained access control to secrets, ensuring that access is granted strictly on a need-to-know basis. f. **Administrator Access.** Administrator access is the responsibility of the CTO, ensuring tight oversight and accountability for sensitive operations. g. **Authorisation of parcelLab Services.** Authorisation is enforced at all levels of the respective systems. Access rights are granted or processed based on the user's job responsibilities or on a need-to-know basis. All access requests must be authorised and approved by the applicant's supervisor using formal workflow tools. h. **Trained and Authorised Users.** Access to production systems is granted only to trained users who are explicitly authorised for the respective actions. Access is immediately revoked in the event of termination. i. **Network Security Policies.** parcelLab uses AWS network security policies to	Zugriff auf das VPN ist auf autorisierte Benutzer beschränkt, die über bestimmte Berechtigungen für bestimmte SSH-Gateways verfügen. Zertifikate, die pro Benutzer bereitgestellt werden, sind für den VPN-Zugriff erforderlich und werden während des On- und Offboardings automatisch über unsere Infrastructure-as-Code-Plattform verwaltet. b. **Berechtigungen und Richtlinien.** Berechtigungen und Zugriff innerhalb des VPN unterliegen strengen Richtlinien und benutzerspezifischen Kontrollen. Diese stellen sicher, dass nur Benutzer mit entsprechenden Rollen auf kritische Ressourcen zugreifen können. c. **Datenbanksicherheit**. Datenbanken innerhalb der VPNs sind verschlüsselt und mit starken Passwörtern geschützt. Unser Infrastructure-as-Code-Ansatz ermöglicht die sichere Verwaltung und Rotation von Datenbankpasswörtern und ermöglicht so ein schnelles Handeln bei Sicherheitsvorfällen. d. **Bereitstellung und Löschung**. parcelLab folgt einem formalen Prozess für die Bereitstellung und Löschung von Benutzerkonten. Zugriffsberechtigungen werden über Gruppenmitgliedschaften verwaltet, eindeutige Benutzer-IDs, sichere

control and restrict access to only the necessary ports and services. Modifications to these rules are limited to a small, technically skilled team. The security team regularly reviews and updates critical security group rules to ensure compliance and security.	Kennwörter und MFA werden erzwungen, um einen sicheren Zugriff zu gewährleisten.
2.3 Data Access Control. To ensure that only authorised individuals can access, copy, alter, or delete specific data, parcelLab implements the following measures to limit access based on each user's permissions:	e. **Kennwortbasierte Authentifizierung.** Für Anwendungen, die SSO nicht unterstützen, verwendet parcelLab branchenübliche Passwortverwaltungssysteme, die eine fein abgestufte Zugriffskontrolle auf Geheimnisse unterstützen und sicherstellen, dass der Zugriff streng nach dem Need-to-know-Prinzip gewährt wird.
2.3.1 Granular Authorisation Systems. parcelLab's systems provide a fine-grained authorisation control, restricting data access based on group memberships, roles, and permissions. Special permissions are required administering these controls, where for the Customer or parcelLab employee accounts.	f. **Administrator-Zugriff.** Der Administratorzugriff liegt in der Verantwortung des CTO, um eine strenge Aufsicht und Verantwortlichkeit für sensible Vorgänge zu gewährleisten.
2.3.2 Logging. All access and changes to permissions, as well as user login activity, are logged as an internal audit log to ensure traceability and accountability.	g. **Autorisierung von parcelLab Services.** Die Autorisierung wird auf allen Ebenen der jeweiligen Systeme durchgesetzt. Zugriffsrechte werden auf der Grundlage der beruflichen Verantwortlichkeiten des Benutzers oder auf einer Need-to-know-Basis gewährt oder verarbeitet. Alle Zugangsanträge müssen vom Vorgesetzten des Antragstellers unter Verwendung formaler Workflow-Tools genehmigt werden.
2.3.3 SSO Support and Recommendations. parcelLab supports and recommends SSO integrations to its Customers that allow authentication through the Customer's identity management systems. Authorisation can also be managed via the SSO integration to provide a seamless and secure access control experience.	h. **geschulte und autorisierte Benutzer.** Der Zugriff auf Produktivsysteme wird nur geschulten Benutzern gewährt, die explizit für die
2.4 Handover Control. To ensure that data cannot be read, copied, altered, removed without authorisation during electronic transmission, transport, or storage on data carrier, parcelLab implements the following measures:	
2.4.1 Secure Data Transmission. Establishment of VPN tunnels to ensure secure electronic data transmission.	
2.4.2 Audit Logs and Automated Deletions. (Anonymous) logging of all exports,	

modifications, or deletions performed on behalf of the Customer. Data deletions are executed automatically at agreed intervals.

2.4.3 **Process Transparency.** Creation of an overview of regular data retrieval and transmission processes for the Customer.

2.4.4 **Anonymisation and Pseudonymisation.** Data is passed on in an anonymised or pseudonymized form whenever feasible.

2.4.5 **Data Encryption.** parcelLab employs robust encryption protocols to protect data during transmission and storage.

2.4.6 **Access Controls for Sensitive Systems.** Access to systems used for data evaluation and anonymisation is subject to strict access controls, as described in Section 2.3, above.

2.4.7 **Employee Awareness and Incident Reporting.** Employees are trained to understand the risks associated with cloud-based services. All Employees are bound by strict NDAs and are required to report the loss or theft of any device containing sensitive data to parcelLab.

2.5 **Deletion of Data.** The time and frequency of data deletion is determined by the Customer, subject to the requirements of the Agreement. By default, parcelLab automatically deletes all End-User Personal Data used for processing on a rolling basis after 90 days. This default retention period can be extended upon Customer request to align with a customer-defined retention schedule.

2.6 **Separation Control.** parcelLab ensures the separate processing of data collected for different purposes through its multi-customer capability.

jeweiligen Aktionen autorisiert sind. Im Falle einer Kündigung wird der Zugang sofort gesperrt.

i. **Richtlinien für die Netzwerksicherheit.** parcelLab verwendet AWS-Netzwerksicherheitsrichtlinien, um den Zugriff auf die erforderlichen Ports und Services zu kontrollieren und einzuschränken. Änderungen an diesen Regeln sind auf ein kleines, technisch versiertes Team beschränkt. Das Sicherheitsteam überprüft und aktualisiert regelmäßig kritische Regeln für Sicherheitsgruppen, um Compliance und Sicherheit zu gewährleisten.

2.3 **Kontrolle des Datenzugriffs.** Um sicherzustellen, dass nur autorisierte Personen auf bestimmte Daten zugreifen, sie kopieren, ändern oder löschen können, implementiert parcelLab die folgenden Maßnahmen, um den Zugriff auf der Grundlage der Berechtigungen jedes Benutzers einzuschränken:

2.3.1 **Granulare Berechtigungssysteme.** Die Systeme von parcelLab bieten eine fein abgestufte Berechtigungssteuerung, die den Datenzugriff auf Basis von Gruppenmitgliedschaften, Rollen und Berechtigungen einschränkt. Für die Verwaltung dieser Kontrollen sind spezielle Berechtigungen erforderlich, die für das Kunden- oder parcelLab-Mitarbeiterkonto gelten.

2.3.2 **Protokollierung.** Alle Zugriffe und Änderungen an Berechtigungen sowie die Anmeldeaktivitäten der Benutzer werden im internen Audit-Protokoll erfasst, um die

	Nachvollziehbarkeit und Verantwortlichkeit zu gewährleisten. **2.3.3** **SSO-Unterstützung und Empfehlungen.** parcelLab unterstützt und empfiehlt seinen Kunden SSO-Integrationen, die eine Authentifizierung über die Identitätsmanagementsysteme des Kunden ermöglichen. Die Autorisierung kann auch über die SSO-Integration verwaltet werden, um eine nahtlose und sichere Zutrittskontrolle zu gewährleisten. **2.4** **Kontrolle der Datenübertragung.** Um sicherzustellen, dass Daten während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt werden können, ergreift parcelLab folgende Maßnahmen: **2.4.1** **Sichere Datenübertragung.** Einrichtung von VPN-Tunneln, um eine sichere elektronische Datenübertragung zu gewährleisten. **2.4.2** **Überwachungsprotokolle und automatisierte Löschvorgänge.** (Anonyme) Protokollierung aller Exporte, Modifikationen oder Löschungen, die im Auftrag des Kunden durchgeführt wurden. Datenlöschungen werden automatisch in vereinbarten Intervallen durchgeführt. **2.4.3** **Transparenz im Prozess.** Erstellung einer Übersicht über die regelmäßigen Datenabruf- und -übertragungsvorgänge für den Kunden. **2.4.4** **Anonymisierung und Pseudonymisierung.** Die Weitergabe der Daten erfolgt, wann immer möglich, in anonymisierter oder pseudonymisierter Form. **2.4.5** **Datenverschlüsselung.** parcelLab verwendet robuste

	Verschlüsselungsprotokolle, um Daten während der Übertragung und Speicherung zu schützen. **2.4.6 Zugriffskontrollen für sensible Systeme.** Der Zugriff auf Systeme, die zur Datenauswertung und Anonymisierung verwendet werden, unterliegt strengen Zugriffskontrollen, wie oben in Abschnitt 2.3 beschrieben. **2.4.7 Sensibilisierung der Mitarbeiter und Meldung von Vorfällen.** Die Mitarbeiter werden geschult, um die mit Cloud-basierten Diensten verbundenen Risiken zu verstehen. Alle Mitarbeiter sind an strenge NDAs gebunden und verpflichtet, den Verlust oder Diebstahl von Geräten, die sensible Daten enthalten, an parcelLab zu melden. **2.5 Löschung von Daten.** Der Zeitpunkt und die Häufigkeit der Datenlöschung werden vom Kunden vorbehaltlich der Anforderungen des Vertrags festgelegt. Standardmäßig löscht parcelLab automatisch alle personenbezogenen Endnutzerdaten, die für die Verarbeitung verwendet werden, fortlaufend nach 90 Tagen. Dieser standardmäßige Aufbewahrungszeitraum kann auf Kundenwunsch verlängert oder verkürzt werden, um ihn an einen vom Kunden definierten Aufbewahrungsplan anzupassen. **2.6 Steuerung der Datentrennung.** parcelLab stellt durch seine Mandantenfähigkeit die getrennte Verarbeitung der zu unterschiedlichen Zwecken erhobenen Daten sicher.
3. Integrity. **3.1 Transfer Control.** No unauthorised reading, copying, modification or removal during electronic transmission or transport by encryption via https (hypertext transfer protocol secure).	**3. Integrität.** **3.1 Übertragungssicherheit** Kein unbefugtes Auslesen, Kopieren, Verändern oder Entfernen bei der elektronischen Übertragung oder dem Transport durch Verschlüsselung über https (Hypertext Transfer Protocol Secure).

3.2 Input Control. Document management and logging track who has added, changed, or removed personal data in the data processing systems.	**3.2 Eingabekontrolle.** Dokumentenmanagement und Protokollierung verfolgen, wer personenbezogene Daten in den Datenverarbeitungssystemen hinzugefügt, geändert oder entfernt hat.
4. Availability. **4.1 Ensuring Availability.** parcelLab protects against accidental or deliberate destruction or loss of data through a robust backup strategy and firewall protections, ensuring rapid recoverability as required under Article 31(1)(c) of the GDPR. The backup strategy for the primary database cluster includes three levels of protection: i. **Multi-Availability Zone Redundancy.** The primary database cluster operates with hot redundancy and continuous backup to separate nodes; ii. **Hourly Backups.** Automatic image-level backups are performed hourly, enabling in less than 10 minutes; and iii. **Daily Off-Site Backups.** Off-site backups are created daily for disaster cases. All primary systems, including the API, operate in triple hot redundancy across three availability zones. **4.2 Earmarking.** The subject matter of parcelLab's engagement includes the Services, work and/or performances described and agreed in more detail in the Agreement.	**4. Verfügbarkeit.** **4.1 Sicherstellung der Verfügbarkeit.** parcelLab schützt vor versehentlicher oder vorsätzlicher Zerstörung oder Verlust von Daten durch eine robuste Backup-Strategie und Firewall-Schutzmaßnahmen, die eine schnelle Wiederherstellbarkeit gemäß Artikel 31 Absatz 1 Buchstabe c der DSGVO gewährleisten. Die Sicherungsstrategie für den primären Datenbankcluster umfasst drei Schutzstufen: i. **Redundanz in Multi-Availability-Zonen.** Der primäre Datenbankcluster arbeitet mit Hot-Redundanz und kontinuierlicher Sicherung auf separaten Knoten. ii. **Stündliche Backups.** Automatische Backups auf Image-Ebene werden stündlich durchgeführt und ermöglichen dies in weniger als 10 Minuten. iii. **Tägliche Offsite-Backups.** Offsite-Backups werden täglich für Katastrophenfälle erstellt. Alle primären Systeme, einschließlich der API, arbeiten in dreifacher Hot-Redundanz über drei Verfügbarkeitszonen hinweg. **4.2 Zweckbindung.** Gegenstand des Auftrags von parcelLab sind die Leistungen, Arbeiten und/oder Leistungen, die im Vertrag näher beschrieben und vereinbart werden.
5. Load Capacity of the Systems. parcelLab's systems are designed to dynamically scale based on load and performance metrics within cloud environments. Capacity limits are proactively managed to ensure system availability, and scaling actions are monitored for early	**5. Belastbarkeit der Systeme.** Die Systeme von parcelLab sind so konzipiert, dass sie dynamisch auf der Grundlage von Last- und Leistungsmetriken innerhalb von Cloud-Umgebungen skaliert werden können. Kapazitätsgrenzen werden proaktiv verwaltet, um die Systemverfügbarkeit

intervention, when necessary, where not done automatically.	sicherzustellen, und Skalierungsaktionen werden überwacht, um bei Bedarf frühzeitig eingreifen zu können, wenn dies nicht automatisch geschieht.
6. Recovery After Incident. Redundant backup servers are implemented to support rapid recovery and ensure data availability (see Section 4.1 above).	**6. Wiederherstellung nach einem Vorfall.** Redundante Backup-Server werden implementiert, um eine schnelle Wiederherstellung zu unterstützen und die Datenverfügbarkeit sicherzustellen (siehe Abschnitt 4.1 oben).
7. Regular Review of TOMs. parcelLab conducts regular reviews of its TOMs, including data protection management, incident-response-management, and data protection-friendly default settings, in accordance with Article 25(2) of the GDPR	**7. Regelmäßige Überprüfung der TOMs.** parcelLab führt gemäß Art. 25 Abs. 2 DSGVO regelmäßige Überprüfungen seiner TOMs durch, einschließlich Datenschutzmanagement, Incident-Response-Management und datenschutzfreundliche Voreinstellungen
8. Documentation. Documentation serving as proof of the orderly and proper processing of End-User Customer Data is securely stored beyond the end of the Agreement, in compliance with application retention periods.	**8. Dokumentation.** Dokumentationen, die als Nachweis für die ordnungsgemäße Verarbeitung von Endkundendaten dienen, werden über das Ende des Vertrags hinaus unter Einhaltung der Aufbewahrungsfristen für Anwendungen sicher aufbewahrt.