parcelLab

Data Processing Agreement (EN)

Applicable to parcelLab's Master Service Agreement

Version 5.0

May 2025

parcelLab

Data Processing Agreement

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**").

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.

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 processing 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 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.

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.

3.2 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.

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.

3.4 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.

3.5 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.

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, 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.

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.

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 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.

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.

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.

8.2 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

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.

8.4 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.

9. DELETION AND RETURN OF PERSONAL DATA

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 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.

10. DATA PROTECTION OFFICER

Processor has appointed an external Data Protection Officer (DPO) who can be reached at dataprotection@parcellab.com

Appendix 1

Technical and Organisational Measures (TOMs)

parcelLab undertakes to implement the following technical and organisational measures in accordance with Article 28(3)(2)(c) and Article 32 of the GDPR.

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.

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/
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 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.

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.

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 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.

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:

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.

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.

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.

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.

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).

3.2 Input Control. Document management and logging track who has added, changed, or removed personal data in the data processing systems.

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.

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 intervention, when necessary, where not done automatically.

6. **Recovery After Incident.**
   Redundant backup servers are implemented to support rapid recovery and ensure data availability (see Section 4.1 above).

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.

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.