Data Protection Terms and Information Security Policy

Overseas Courier Service (London) Ltd
Effective Date: 30th June 2025

1. Purpose

This Policy sets out how Overseas Courier Service (London) Ltd ("OCS") collects, processes, stores, transfers, and protects Personal Data in accordance with the UK GDPR, the Data Protection Act 2018 (DPA 2018), and other applicable Data Protection Laws.

The Policy also outlines the technical and organisational measures in place to ensure confidentiality, integrity, availability, and resilience of information, particularly in relation to services provided to international ecommerce clients.

2. Scope

This Policy applies to:

- All Personal Data processed by OCS as a Data Processor or Data Controller (as applicable).
- All employees, contractors, agents, and authorised Sub-Processors of OCS.
- All systems, platforms, networks, and facilities where Personal Data is stored or processed.

3. Definitions

- **Personal Data**: As defined by the GDPR and DPA 2018.
- **Data Subject**: Any individual whose Personal Data is processed.
- **Data Controller**: The party determining the purposes and means of processing.
- **Data Processor**: The party processing data on behalf of a Data Controller.
- **Personal Data Breach**: Any unauthorised access, loss, alteration, or disclosure of Personal Data.

4. Roles & Responsibilities

- OCS acts primarily as a Data Processor on behalf of its ecommerce clients (Data Controllers).
- A Data Protection Officer (DPO) or nominated Data Protection Lead shall oversee compliance.
- All employees handling Personal Data are responsible for compliance with this Policy and undergo mandatory training.

5. Data Protection Principles

In compliance with Article 5 of the GDPR, OCS ensures that Personal Data is:

1. **Lawful, fair, and transparent** – processed only on documented lawful bases and communicated to Data Subjects where required.
2. **Limited to purpose** – collected only for explicit and legitimate purposes.
3. **Data minimisation** – restricted to what is necessary.
4. **Accurate** – kept up to date and rectified when necessary.
5. **Storage-limited** – retained no longer than required.
6. **Secure** – protected with appropriate technical and organisational measures.

6. Processing of Personal Data

OCS will:

- Only process Personal Data in accordance with written instructions from the Client (Controller).
- Ensure processing is limited to the services agreed
- Maintain clear records of processing activities (Article 30 GDPR).
- Not use Personal Data for its own purposes.

7. Sub-Processing

- Sub-Processors must be bound by contractual obligations on data protection and confidentiality, subject to local laws and customs.
- OCS remains fully liable for Sub-Processor compliance.

8. Information Security Controls

OCS maintains and reviews regularly a suite of technical and organisational security measures (TOMs), including but not limited to:

Technical Measures

- Encryption of Personal Data in transit (TLS/SSL).
- Separated client data within systems.
- Vulnerability assessments, penetration testing, and patch review and management.
- Monitoring, alerting, and logging of access attempts.

Organisational Measures

- Strict role-based access controls (least privilege principle).
- Confidentiality agreements with all personnel handling Personal Data.
- Business continuity and disaster recovery planning to ensure resilience.

9. Data Subject Rights

- OCS will record and promptly notify Clients of any Data Subject requests (access, rectification, erasure, restriction, portability, objection).
- No Data Subject requests will be actioned without prior approval and instruction from the Client.
- OCS will support the Client in meeting response deadlines required by law.

10. Personal Data Breach Management

- Any suspected or actual breach will be reported to the Client within 24 hours of becoming aware.
- Breach reports will include the nature, scope, affected data, risks, and remedial actions.
- No external announcements will be made without Client approval, unless required by law.

11. International Transfers

- Personal Data will not be transferred outside the UK or EEA unless:
- The transfer is to an Adequate Country, or
- The transfer is subject to approved Standard Contractual Clauses (SCCs) and/or the UK International Data Transfer Addendum (IDTA).
- OCS ensures protections are applied to all overseas processing where permitted.

12. Audits & Cooperation

- OCS will maintain records of processing and security measures.
- Clients (or authorised auditors) may audit compliance with this Policy on reasonable notice.
- OCS will cooperate with the ICO and other Supervisory Authorities as required.

13. Retention & Deletion

- Personal Data is retained only for as long as necessary to provide services or meet legal obligations.
- On termination of services, all Personal Data will be securely deleted unless retention is legally required.

14. Complaints & Liability

- OCS will promptly notify Clients of any Complaints received from Data Subjects or Supervisory Authorities.
- OCS shall indemnify Clients against losses caused by breaches of this Policy, subject to the terms of the Main Agreement.

15. Governance & Review

- This Policy will be reviewed annually or earlier if legal, regulatory, or operational changes require.
- Updates will be communicated to all staff and Clients.

Appendix A – Description of Processing

1. Subject Matter of Processing

The processing of Personal Data by OCS is carried out in connection with the provision of international ecommerce distribution, courier, and fulfilment services to the Client.

2. Nature and Purpose of Processing

The processing may include the following activities:

- Receiving, storing, and handling customer order data for the purpose of shipping and fulfilment.
- Printing, packaging, and dispatching orders to customers.
- Tracking and updating delivery status.
- Managing returns, exchanges, or failed deliveries.
- Providing customer service support relating to shipping and delivery.
- Securely transmitting shipping and tracking data to customs authorities, couriers, and delivery partners as required by law.

3. Categories of Personal Data

The Personal Data processed may include, but is not limited to:

- Customer full name.
- Contact details (postal address, email address, telephone number).
- Order details (order number, product(s) purchased, order value, currency).
- Delivery and tracking information.
- Customer service correspondence relating to deliveries.

No special category Personal Data (Article 9 GDPR) is intended to be processed.

4. Categories of Data Subjects

The Personal Data processed relates to:

- End Customers of the Client (i.e., individual purchasers of goods via ecommerce platforms).
- Client Personnel (limited to authorised contacts for operational purposes such as shipping, account management, and reporting).

5. Duration of Processing

- OCS will retain and process Personal Data only for as long as necessary to fulfil the Client's instructions, meet contractual obligations, and comply with applicable legal or regulatory requirements.
- Data will be securely deleted upon termination of services, unless retention is required by law.

6. Data Transfers

- Personal Data may be transferred to couriers, logistics providers, and customs authorities located within and outside the UK/EEA, strictly for the purpose of fulfilling deliveries.
- Any transfer outside the UK/EEA will be subject to appropriate safeguards, including Adequacy Decisions, Standard Contractual Clauses (SCCs), and/or the UK IDTA.

7. Authorised Sub-Processors

The following categories of Sub-Processors may be engaged, subject to Client approval:

- **IT service providers** (hosting, infrastructure, data storage).
- **Courier and logistics partners** (domestic and international).
- **Customer service support providers** (if engaged).
- **Regulatory or customs authorities** (where legally required).

8. Security Measures

OCS maintains technical and organisational measures (TOMs) to protect Personal Data, including:

- Encryption in transit.
- Role-based access controls.
- Confidentiality undertakings for personnel.
- Penetration testing and system monitoring.
- Business continuity and disaster recovery plans.