



# Data Privacy Policy Compliance Checklist

## Data Mapping & Inventory

Identify all data collected, processed, and stored within logistics operations. This includes data related to customers, employees, vendors, delivery locations, and goods.

**Describe all types of personal data collected related to customers (e.g., name, address, contact details, order history, tracking information).**

Write something...

**Describe all types of personal data collected related to employees (e.g., name, address, contact details, payroll information, performance data).**

Write something...

**Describe all types of personal data collected related to vendors/suppliers (e.g., contact details, payment information, contract terms).**

Write something...

### Which data categories are collected via website/app forms?

- ☐ Name
- ☐ Email Address
- ☐ Phone Number
- ☐ Delivery Address
- ☐ Payment Information
- ☐ Order History
- ☐ Location Data
- ☐ Other (Specify in LONG\_TEXT)


### Estimated number of customer records stored.

Enter a number...

### Primary method of data storage (e.g., cloud database, on-premise servers, spreadsheets).

- ☐ Cloud Database
- ☐ On-Premise Servers
- ☐ Spreadsheets
- ☐ Other (Specify in LONG\_TEXT)

### Upload a diagram or flow chart illustrating data flow within logistics operations.

 Upload File

## Consent & Notice

Ensure compliance with consent requirements for data collection and processing, and provide clear and transparent privacy notices to relevant parties (customers, employees, vendors).

## Draft Customer Privacy Notice for Logistics Services

Write something...


## Consent Method for Customer Data Collection (e.g., opt-in, implied consent)

- ☐ Explicit Opt-in
- ☐ Implied Consent
- ☐ Other (Specify)

## Summary of Key Information Provided in Privacy Notice (to ensure clarity)

Write something...

## Example Customer Consent Form (if applicable)

 Upload File

## Method of Providing Notice to Customers (e.g., website, email, in-person)

- ☐ Website
- ☐ Email
- ☐ In-Person
- ☐ Other (Specify)

## Date Last Updated Customer Privacy Notice

Enter date...

# Data Subject Rights Management

Establish procedures to handle data subject requests, including access, rectification, erasure, restriction of processing, and data portability.

## Data Subject Request Type

- ☐ Access Request
- ☐ Rectification Request
- ☐ Erasure Request ('Right to be Forgotten')
- ☐ Restriction of Processing Request
- ☐ Data Portability Request
- ☐ Objection to Processing Request

## Data Subject Request Details

Write something...

## Data Subject Identification Information

Write something...

## Request Received Date

Enter date...

## Response Deadline

Enter date...

### Response Sent Date

Enter date...

### Response Status

- ☐ In Progress
- ☐ Completed
- ☐ Rejected
- ☐ Pending Verification

### Response Details / Explanation

Write something...

### Supporting Documentation

 Upload File

## Data Security & Protection

Implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, alteration, or destruction throughout the logistics lifecycle.

### Encryption Strength (in bits)

Enter a number...

### Data Security Measures Implemented (Select all that apply)

- ☐ Encryption at Rest
- ☐ Encryption in Transit (TLS/SSL)
- ☐ Firewalls
- ☐ Intrusion Detection/Prevention Systems
- ☐ Access Controls (Role-Based)
- ☐ Data Loss Prevention (DLP)
- ☐ Regular Security Audits

### Description of Physical Security Measures for Warehouses/Distribution Centers

Write something...


### Type of Access Control Used

- ☐ Role-Based Access Control (RBAC)
- ☐ Attribute-Based Access Control (ABAC)
- ☐ Other

### Date of Last Vulnerability Scan

Enter date...

### Upload Results of Latest Penetration Testing Report

 Upload File

### Number of Failed Login Attempts Before Account Lockout

Enter a number...

### Detailed Description of Data Masking or Pseudonymization Techniques Used (if applicable)

Write something...

## Vendor & Third-Party Management

Assess and manage the data privacy practices of all vendors and third-party providers involved in logistics operations (e.g., transportation providers, warehouse management systems, delivery services).

### Vendor Privacy Risk Assessment Performed?

- ☐ Yes
- ☐ No
- ☐ N/A

### Summary of Vendor Data Processing Activities

Write something...

### Vendor Privacy Policy/Agreement

 Upload File

### Vendor Data Processing Agreement (DPA) in Place?

- ☐ Yes
- ☐ No
- ☐ N/A

### Description of Vendor Security Measures

Write something...

### Number of Vendors Requiring Ongoing Monitoring

Enter a number...

### Data Categories Processed by Vendors (Select All That Apply)

- ☐ Customer Data
- ☐ Employee Data
- ☐ Location Data
- ☐ Vehicle Data
- ☐ Financial Data
- ☐ Other

### Date of Last Vendor Privacy Assessment

Enter date...

## Cross-Border Data Transfers

Address compliance requirements for transferring personal data across international borders, ensuring adherence to relevant regulations (e.g., GDPR, CCPA).



**Are cross-border data transfers required for logistics operations?**

☐ Yes

☐ No

**Which countries do data transfers occur to?**

☐ United States

☐ Canada

☐ United Kingdom

☐ Germany

☐ China

☐ Australia

☐ Japan

☐ Other (Specify in LONG\_TEXT)

**If 'Other' selected above, specify the countries:**

Write something...

**What transfer mechanism is used (e.g., SCCs, Binding Corporate Rules, Adequacy Decision)?**

☐ Standard Contractual Clauses (SCCs)

☐ Binding Corporate Rules (BCRs)


☐ Adequacy Decision

☐ Other (Specify in LONG\_TEXT)

**If 'Other' selected above, specify the transfer mechanism:**

Write something...

**Upload documentation of the transfer mechanism (e.g., SCCs copy, BCR approval document)**

 Upload File

**Describe the data minimization and pseudonymization measures in place for cross-border transfers.**

Write something...

**Date of last review/update of cross-border transfer documentation.**

Enter date...

## Employee Training & Awareness

Provide regular training to employees on data privacy policies, procedures, and best practices related to logistics operations.

**Have you reviewed the latest Data Privacy Policy?**

- ☐ Yes
- ☐ No
- ☐ Not Started

**Briefly describe your understanding of key data privacy principles (e.g., data minimization, purpose limitation).**

Write something...

**Which types of personal data do you regularly handle in your role?**

- ☐ Customer Contact Information
- ☐ Delivery Addresses
- ☐ Employee Records
- ☐ Vehicle Tracking Data
- ☐ Vendor Information
- ☐ None

**Are you familiar with the process for reporting a suspected data privacy breach?**

- ☐ Yes
- ☐ No
- ☐ Unsure

**Date of last Data Privacy Training Completion**

Enter date...

**Describe a situation where you had to consider data privacy in your work, and how you handled it.**

Write something...

**Do you know who to contact for data privacy-related questions or concerns?**

- ☐ Yes
- ☐ No
- ☐ Unsure

# Incident Response & Breach Notification

Develop and maintain an incident response plan to address data breaches and ensure timely notification to relevant stakeholders and regulatory bodies as required.

## Date of Incident Discovery

Enter date...

## Time of Incident Discovery

## Detailed Description of Incident

Write something...

## Incident Category (e.g., Malware, Unauthorized Access, Lost Device)

- ☐ Malware Infection
- ☐ Unauthorized Access
- ☐ Lost/Stolen Device
- ☐ Human Error
- ☐ Third-Party Breach
- ☐ Other

## Estimated Number of Records Affected

Enter a number...

### Data Types Involved (e.g., Customer Data, Employee Data)

- ☐ Customer Data
- ☐ Employee Data
- ☐ Vendor Data
- ☐ Logistics Data (Tracking, Inventory)
- ☐ All Data Types

### Containment Steps Taken

Write something...

### Notification Parties Involved (Check all that apply)

- ☐ Customers
- ☐ Employees
- ☐ Vendors
- ☐ Regulatory Bodies (e.g., GDPR Authorities)
- ☐ Law Enforcement
- ☐ Legal Counsel
- ☐ PR/Communications

### Date of Notification to Affected Parties

Enter date...

## Record Keeping & Documentation

Maintain comprehensive records of data processing activities, consent records, privacy notices, risk assessments, and other relevant documentation to demonstrate compliance.

### Last Policy Review Date

Enter date...

### Summary of Changes Made During Last Review

Write something...

### Copy of Current Data Privacy Policy Document

 Upload File

### Number of Data Subject Requests Received (Last 12 Months)

Enter a number...

### Number of Data Subject Requests Successfully Completed (Last 12 Months)

Enter a number...

### Description of Data Processing Agreements with Key Vendors

Write something...

### Types of Personal Data Processed (Select all that apply)

- ☐ Customer Name
- ☐ Customer Address
- ☐ Vehicle Registration
- ☐ Employee Data
- ☐ Delivery Location Coordinates
- ☐ Product Information (if identifying)

### Record of Data Breach Incident Responses (if applicable)

Write something...

### Data Mapping Documentation (e.g., spreadsheet)

 Upload File

## Policy Review & Updates

Establish a process for periodic review and updates to the data privacy policy and associated procedures to reflect changes in regulations, business practices, and technology.

### Last Policy Review Date

Enter date...

### Summary of Changes Made During Review

Write something...


**Frequency of Policy Review (in months)**

Enter a number...

**Triggering Events for Review (Select All that Apply)**

- ☐ Regulatory Changes
- ☐ Business Process Changes
- ☐ Data Breach/Security Incident
- ☐ New Technologies Implemented
- ☐ Contractual Obligations
- ☐ Audit Findings

**Attach Previous Version of Policy**

 Upload File

**Rationale for Review Frequency**

Write something...

**Next Scheduled Review Date**

Enter date...