Postal.io, Inc.

Data Security & Privacy

1. GLOSSARY OF TERMS

Term/Acronym	Definition
Automated Decision-Making (ADM)	means when a decision based solely on automated processing, including profiling, which produces legal effects or similarly affects a Data Subject.
CCPA	means the California Consumer Privacy Act of 2018.
Confidential Information	means non-public information that derives independent value from not being generally known to the public, but does not include any information that (i) was or subsequently becomes publicly available without breach of any confidentiality obligations, (ii) was known prior to the disclosure of such information, (iii) was or is subsequently obtained from another source without breach of any confidentiality obligation, or (iv) is independently developed without reference to any Sensitive and/or Confidential Information.
Consent	means a statement or a clear affirmative action, performed by the Data Subject, that signifies their agreement to the Processing of their Personal Data. Consent should be freely given, specific, informed, and be an unambiguous indication of the Data Subject's wishes.
Data Breach	*Please refer to the Postal.io' Incident Response Policy.*
Data Controller	means the person or organization that determines the purpose and means of the Processing of Personal Data.
Data Processor	means the person or organization that Processes Personal Data on behalf of the Data Controller.
Data Subject	means an identified or identifiable natural person whose rights are protected by applicable data protection and privacy laws, including, but not limited to, a "Consumer" as defined in the CCPA.

Dispose	and its cognates mean the discarding or abandonment of Sensitive and/or Confidential Information; or the sale, donation, or transfer of any medium, including computer equipment, upon which this Sensitive and/or Confidential Information is stored.
GDPR	means the (a) Regulation (EU) 2016/679 on the protection of natural persons with regard to Processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), and (b) the UK GDPR.
Need to Know Parties (NKP)	means Postal.io consultants, vendors, partners, or other third parties that are provided Information by Postal.io on a need-to-know basis subject to confidentiality obligations.
Personal Data	means any information relating, directly or indirectly, to an identified or identifiable Data Subject, where such information is protected under applicable law or regulation.
Personal Identifiable Information (PII)	means a Data Subject's first name or first initial and last name in combination with any one or more of the following data elements: (i) social security number; (ii) driver's license number or state-issued identification card number; or (iii) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to a Data Subject's financial account.
Personnel	means Postal.io employees (part-time and full-time), interns, directors, and members.
Process	and its cognates mean any operation or set of operations which is performed on Personal Data, whether or not by automatic means, such as collection, recording organization, structuring, storage, adaption or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	means a specific NKP that Processes Personnel Data with respect to Postal.io' corporate operations.

Security Incident	*Please refer to the Postal.io' Incident Response Policy.*
Sensitive Information	means to Personal Data, PII, and SPD.
Sensitive Personal Data (SPD)	is a form of Personal Data and means any information revealing a Data Subject's genetic or biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation and lifestyle, or criminal convictions or offenses.
Subject Access Request (SAR)	means request made by or on behalf of a Data Subject for information which they are entitled to ask for under applicable law or regulation, including, but not limited to, the GDPR, the UK GDPR or the CCPA.
Subprocessor	means a specific NKP that processes subscriber Personal Data in connection with any product or service delivered by Postal.io, including the Postal.io Talent Platform.
Subscriber Data	*Please refer to the Postal.io Subscription Agreement*
UK GDPR	means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

2. POSTAL.IO'S COMMITMENT TO PRIVACY

Postal.io, Inc. ("Postal.io") recognizes the importance of protecting and ensuring the integrity of Sensitive and Confidential Information, including Personal Data. Sensitive and Confidential Information is gathered, used, stored, shared, secured, retained, and disposed of in accordance with applicable laws and regulations, privacy best practices, and the terms of the agreement between Postal.io and the subscriber.

This Data Security & Privacy Statement ("Statement") explains how we process, gather, use, store, share, secure, retain, and dispose of Sensitive and Confidential information, including Personal Data, on behalf of our subscribers' and their users. To this end, Postal.io has adopted this statement and program designed to secure and limit unauthorized disclosure of such confidential, proprietary, and/or Personal Data.

Data Transfers

We ask clients to sign our Data Processing Addendum for cross-border data transfers. The DPA includes Standard Contractual Clauses to cover the data transfer and handling of your data.

3. WHO ARE WE?

Postal.io delivers a tool that allows subscribers to send corporate gift, direct mail and other 'offline' offerings for sales & marketing purposes or as determined by the subscriber. Postal.io is dedicated to meeting the privacy and data protection needs of its subscribers, in order to protect Sensitive and Confidential Information for our subscribers' users.

4. TYPES OF SENSITIVE INFORMATION PROCESSED

Postal.io processes information on behalf of its subscribers. The type of information generally processed by Postal.io includes the following categories of data.

- First Name
- Last Name
- Work Address
- Email Address

To this end, Postal.io recognizes that processing Sensitive Information varies by country and implements the following principles of data protection based upon the agreement between the subscriber and Postal.io, and the subscriber's requirements.

- Personal Data

Postal.io processes Personal Data as defined by the EU GDPR on behalf of its subscribers. Personal Data includes the following data types: Electronic Data.

Examples of Types of Personal Data

Internal Data	External Data	Financial Data
• Religious or Philosophical Beliefs • Passwords • PINs	• Name • Username • Unique Identifier • Gov't Issued Identification	• Credit Card Number • Bank Account Number • Automobile Ownership

• Mother's Maiden Name • Opinions • Intentions • Interests • Likes/Dislikes	• Picture • Biometric Data • Ethnicity/Race • Spoken Language • Sex Life or Orientation • Browsing Behavior • Call Logs • Links Clicked • Demeanor/Attitude • Demographic Information • Medical or Health Information • Physical Characteristics	• Home Ownership • Apartment Rentals • Personal Possessions • Credit Report • Sales and Purchases • Loan Records • Spending Habits • Taxes • Credit Worthiness • Credit Score • Credit • Capacity

Social Data	**Historical Data**	Electronic Data
• Job Titles • Work History • School Attended • Employee Records • Employment History • Evaluations • References • Interviews • Certifications • Disciplinary Actions	Information about an individual's personal history (e.g., whether they were part of 9/11, WWI, WWII)	• IP Address • MAC Address • Browser Fingerprint • Email Address • Physical Address • Telephone Number • Country • GPS coordinates • Electronic Room Number

5. HOW WE PROCESS CONFIDENTIAL AND SENSITIVE INFORMATION

Personnel and NKPs shall only use Confidential and Sensitive Information for a legitimate business purpose in the performance of their duties, including (without limitation):

- To provide the Subscription to subscribers and their users or as otherwise permitted by a subscriber in its agreement with Postal.io;
- To support Postal.io's quality, security, and customer experience improvement initiatives.

5.1. Processing of Personal Data

Postal.io recognizes the importance of processing Personal Data, and values the lawful, accurate, and secure processing of Personal Data. Therefore, to assist its subscribers in complying with applicable laws and regulations, Postal.io's Subscription is enabled to Process Personal Data on behalf of its subscribers and in accordance with the following Data Protection Principles:

1. Personal Data is obtained and Processed fairly and lawfully and shall not be Processed unless the Processing is necessary for the purposes defined under applicable data protection and privacy law or regulation, including, but not limited to, the GDPR.
2. Personal Data is obtained for one or more lawful purposes and not Processed in a manner incompatible with that purpose.
3. Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are Processed.
4. Personal Data is accurate and kept up to date.
5. Personal Data should not be kept for longer than is necessary for that purpose.
6. Personal Data shall be Processed in accordance with the rights of the Data Subject.

These Data Protection Principles must be followed at all times when Processing or using Personal Data.

Through appropriate management and strict application of criteria and controls, Postal.io by and through the Postal.io Subscription:

1. Observes the fair collection and use of Personal Data by collecting consent or providing notice about the legitimate grounds for Processing Personal Data.
2. Delivers notification of how Personal Data is Processed at the time it is collected from a Data Subject.
3. Provides notification to a Data Subject, explaining the details required to Process their Personal Data.
4. Does not Process Personal Data using ADM.
5. Ensures that Data Subject rights can be fully exercised under applicable law or regulation, including, but not limited to, the GDPR, the UK GDPR (if in force), and the CCPA.
6. Processes Personal Data to fulfill only business and operational requirements.
7. Informs a Data Subject if their Personal Data is to be used in a new way.
8. Ensures that sharing of Personal Data with third parties is subject to formal information sharing protocols and agreements.
9. Transfers Personal Data to Processors and Subprocessors only under circumstances where the Personal Data is adequately protected.
10. Documents all requests and disclosures of Personal Data.

11. Ensures information shared through partnership arrangements will be governed by a data sharing agreement or where the Data Subject has authorized disclosure through a mandate.
12. Discloses Personal Data for a stated purpose.

Lastly, where Postal.io processes Personal Data on behalf of its subscribers, Postal.io serves as a Service Provider as defined in CCPA Section 1798.140(v). Under those same circumstances, Postal.io' subscribers are considered to be a Business as defined in CCPA Section 1798.140(c).

As such, subscribers disclose Personal Data to Postal.io solely for: (i) a valid business purpose; and (ii) Postal.io to provide the Subscription. Except as agreed upon in writing by Postal.io and each subscriber, Postal.io is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Subscription; and (iii) retaining, using, or disclosing the Personal Data outside of the Subscription Agreement between Postal.io and subscriber.

Under no circumstances envisioned in the Subscription Agreement is either party considered to be a Third Party as defined in CCPA Section 1798.140(w).

5.2. Subject Access Rights

Under the applicable law or regulation, including, but not limited to the GDPR, the UK GDPR (if in force), and the CCPA, a Data Subject may request details about his/her Personal Data which Postal.io processes on behalf of a subscriber. These rights may include: the right to be informed that processing is being undertaken, to access one's Personal Data, to prevent processing in certain circumstances, and to correct, rectify, block, or erase Personal Data.

Postal.io assists its subscribers in fulfilling Subject Access Requests in accordance with the terms of the agreement between Postal.io and the subscriber.

5.3. Privacy By Design

Postal.io embeds privacy considerations into business processes and systems through appropriate physical, technological, and procedural controls reasonably designed to ensure Personal Data is processed and secured in accordance with applicable law or regulation, including, but not limited to, the GDPR, the UK GPDR (if in force), and the CCPA.

Postal.io implements various security measures through its information security policies and procedures that ensures that unauthorized access or disclosure of Sensitive and/or Confidential Information does not happen by accident or design.

6. SAFEGUARDING OF CONFIDENTIAL AND SENSITIVE INFORMATION

In addition to processing Personal Data in accordance with the principles provided for in the Section titled, "Types of Sensitive Information Processed," Postal.io adheres to the below data privacy principles for all Sensitive and/or Confidential Information, including PII and SPD. To this end Postal.io, implements physical, procedural, and information technology safeguards as follows:

1. Postal.io implements physical measures to prevent unauthorized entry to our premises and secured areas, as well as unauthorized access to our Sensitive and/or Confidential Information.
2. Postal.io uses an access control system to restrict and monitor the Postal.io premise and secured areas.
3. Postal.io shall use reasonable efforts to ensure all visitors are authorized before entering the Postal.io premises and areas where Sensitive and/or Confidential Information is processed or maintained, including, but not limited to, taking the following actions as appropriate:
    1. Providing visitors a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-Personnel;
    2. Asking visitors to surrender the physical token before leaving the facility or at the date of expiration;
    3. Documenting procedures to help all Personnel easily distinguish between Personnel and visitors, especially in areas where Sensitive Information is accessible.
4. Postal.io shall use reasonable efforts to maintain a physical audit trail of visitor activity, including, but not limited to, documenting the visitor's name, the firm represented, and Personnel authorizing physical access on the log. Logs should be kept for a minimum of three months unless otherwise restricted by law.
5. Access to areas containing sensitive material and stored items, including personal records, financial records, office supplies, and computer equipment are restricted and monitored.
6. Postal.io implements and maintains security practices on its IT systems, including network, equipment, and communication systems supporting Postal.io's internal and remote operations and Postal.io-hosted products and services, including, but not limited to, encryption, virus protection, access controls, firewall egress and ingress, and LAN/WAN security. See **IT Security Policy** for further details.

7. RESPONSIBILITIES OF PERSONNEL

Unauthorized disclosure of Sensitive and Confidential Information is strictly prohibited. Personnel, Processors, and Sub-processors should not disclose Sensitive and Confidential

Information obtained in the course of their work with Postal.io, or access Sensitive and Confidential Information without appropriate permissions. The terms of the agreement between Postal.io and the subscriber dictates how Sensitive and Confidential Information is obtained and/or disclosed.

Personnel shall use reasonable efforts to safeguard Sensitive and Confidential Information and keep it private and confidential, including, but not limited to, taking the following actions as appropriate:

1. Only sharing Information with authorized Personnel and NKP who "need to know" such Information for a legitimate business purpose in the performance of their authorized duties;
2. Only storing all electronic Sensitive and Confidential Information in secured equipment or devices (e.g., using a unique password or biometric security measure for Google Apps login, and/or directory or file access);
3. Only storing paper Sensitive and Confidential Information in a locked drawer or office (i.e., not leaving documents lying openly on desks);
4. Not sharing unique passwords and updating existing passwords on a periodic basis;
5. Properly labeling and/or segregating Sensitive and Confidential Information belonging to one party from information belonging to another party;
6. Not storing any Sensitive Information on any laptop or portable device unless it has been confirmed that such Sensitive Information is encrypted on such equipment or device;
7. Not transmitting any Personal Data and/or Sensitive Personal Information from a non-Postal.io mail server (e.g., personal Gmail, Yahoo!, or Hotmail account).
8. Not leaving any unsecured Sensitive and/or Confidential Information, or unsecured equipment or devices containing Sensitive and/or Confidential Information unattended or in an unsecured area.
9. Using reasonable efforts to Dispose of Sensitive and/or Confidential Information when such Information is no longer needed, and shall obtain the return of Sensitive and/or or Information from an NKP when it no longer needs such Information or it is no longer an authorized NKP.
10. If Personnel encounter information, documents, or other materials, whether disclosed in writing or orally, for which there is some doubt as to whether it should be treated as Confidential or Sensitive Information, or how it can be disclosed or used he or she shall:
    1. Treat such information, documents, or materials as Confidential and/or Sensitive Information as provided herein; and/or
    2. Contact the Executive Team, who shall make a joint determination on how best to proceed.

8. DISPOSAL OF INFORMATION

1. All Sensitive and/or Confidential Information, including Personal Data, PII, and SPD, must be Disposed of in accordance with applicable laws and regulations and Postal.io's policies and procedures that control the Disposal of Sensitive and/or Confidential Information.
2. When Disposing of Information, Personnel and NKPs shall take reasonable measures to protect against unauthorized access to or use of the Information in connection with its Disposal. Examples of such reasonable measures include, but are not limited to, any of the following:
    1. Burning, pulverizing, or shredding of papers or records containing Information so that the Information cannot be practicably read or reconstructed;
    2. Destroying or erasing electronic media containing Information so that the Information cannot practicably be read or reconstructed, consistent with reasonable standards.

9. ACCOUNTABILITY AND LIABILITY

1. The Executive Team shall monitor compliance with this Statement through periodic audits of Postal.io, its Personnel, and NKPs.
2. Any Personnel or NKPs who violate any provision of this Statement may be subject to disciplinary action, up to and including immediate termination of their employment or contractual relationship (as applicable), as is determined appropriate in management's discretion.

10. DATA BACKUP AND DISASTER RECOVERY

Postal.io, through its incident response policies and procedures shall notify the subscriber without undue delay when it becomes aware of a Personal Data Breach affecting the subscribers Personal Data.

Additionally, Postal.io implements an **Incident Response Policy** that ensures a consistent and effective approach to the management of a Security Incident including a Data Breach. Data Breaches usually occur through the unauthorized or accidental use or disclosure of Sensitive and/or Confidential Information by Personnel or by a deliberate attack on the Company's systems.

Security Incidents, including Data Breaches, are handled in accordance with the terms of the agreement between Postal.io and the subscriber and Postal.io's **Incident Response Policy**.