Privacy Compliance Policy (Reg P)

Overview

Priyo Inc. (“[Priyo]” or the “Company”) has developed this Policy to comply with Privacy and Controlling the Assault of Non-Solicited Pornography And Marketing Act (“CAN-SPAM”) requirements.

To ensure that customers are protected against unwanted sharing of their financial information, the Gramm-Leach-Bliley Act (“GLBA”) includes a series of regulations known as the Privacy Rules. The Privacy Rules are intended to ensure the confidentiality and security of consumer and customer information.

When an institution chooses to share customer information, a customer can opt-out, or forbid the sharing of their information. Because we do not share any of our customers' personal information with outside parties (except for the purposes of day-to-day business), it is not necessary for the customer to opt-out. However, we do share information with affiliates, and as required under the Fair Credit Reporting Act, customers are given the opportunity to opt-out.

The GLBA Privacy Rules address the following four concepts:

- Our obligation to inform consumers and customers of our policies and procedures regarding the sharing of their personal information.
- The concept of personal customer information, and the limited exceptions under which we may share this information with outside parties.
- Our responsibilities to protect personal customer information.
- Our responsibility to establish appropriate standards relating to safeguarding customer information.

The three principal requirements of the GLBA Privacy Rules are as follows:

- Provide customers with notices describing our privacy policies and practices, including policies with respect to the disclosure of nonpublic personal information to affiliates and to nonaffiliated third parties.
- Subject to specific exceptions, we may not disclose nonpublic personal information about consumers to any nonaffiliated third party unless consumers are given a reasonable opportunity to direct that such information not be shared (i.e., Opt-Out).
- We generally may not disclose account numbers to any nonaffiliated third party for marketing purposes.

As noted above, Priyo does not share customers’ personal information with nonaffiliated third parties (except for reasons allowed by the Rules), and therefore is not required to provide the customer with the opportunity to opt-out.

The Right to Financial Privacy Act (“RFPA”) establishes specific procedures that federal government authorities must follow in order to obtain information from us about a customer’s financial records. Generally, these requirements include obtaining subpoenas, notifying the customer of the request, and providing the customer with an opportunity to object. The Act imposes related limitations and duties on financial institutions prior to the release of information requested by federal authorities.

The Children’s Online Privacy Protection Act (“COPPA”) was enacted to prohibit unfair and deceptive acts or practices in connection with the collection, use, or disclosure of personal information from children under the age of 13 in an online environment. Generally, the Act requires operators of Websites or online services directed to children, or that have actual knowledge that they are collecting or maintaining personal information from children online, to provide certain notices and obtain parental consent to collect, use, or disclose information about children. The FDIC is granted enforcement authority under the Act. Federal Trade Commission regulations (16 CFR 312) that implement COPPA became effective April 21, 2000.

The California Consumer Privacy Act of 2018 (“CCPA”) gives consumers more control over the personal information that companies collect about them.

The Controlling the Assault of Non-Solicited Pornography And Marketing Act (“CAN-SPAM”) requires Priyo to follow specific procedures when initiating electronic mail (“email”) messages to any recipient with the primary purpose of communicating a commercial message. CAN-SPAM has several requirements related to email messages, including that certain information in email messages is not false or misleading and recipients of commercial messages are able to opt-out of future correspondence.

Policy Statement - CAN SPAM

Priyo is committed to complying with all applicable provisions of CAN-SPAM. Priyo sends email messages to prospective customers as well as to customers where it already has an established business relationship. CAN-SPAM communicates requirements for email messages based on the primary purpose of such email messages.

Policy Statement - Privacy

Priyo seeks to proactively comply with all requirements that stem from regulations that govern our activities. The Privacy Rules within the GLBA apply to all activities that involve nonaffiliated third parties and the disclosure of nonpublic personal information for consumers. Priyo engages with nonaffiliated third parties for the carrying out of financial transactions and for marketing of financial products which includes:

- Vendors that verify consumers' identification information
- Processors that conduct transaction information

- Financial institutions that process financial data

The use of nonpublic personal information for any of these reasons does not require that Priyo obtain explicit prior consent from the consumer. As of the enacting of this policy, Priyo does not engage with any nonaffiliated third party for the purpose of marketing non-financial products to consumers and there are no known plans to do so in the future.

It is the policy of Priyo not to disclose nonpublic personal information about our customers to nonaffiliated third parties except as authorized by law (outlined above). However, Priyo will permit additional information sharing in a manner consistent with legal requirements. To the extent that Priyo seeks to disclose nonpublic information to nonaffiliated third parties in additional circumstances (such as for marketing), Priyo will ensure that the customer is provided with the right to opt-out or limit the sharing by notifying Priyo of such intent through the use of a mail-in form or other permissible means.

Additionally, Priyo aims to comply with the RFPA, which establishes specific procedures that federal government authorities must follow in order to obtain information from a financial institution about a customer's financial records.

Priyo will comply with CCPA requirements for its California consumers.

Should Priyo operate a website or online service directed to children that collects or maintains personal information about them, or knowingly collects or maintains personal information from a child online, the Company will comply with COPPA requirements.

The objective of this Privacy Policy is to protect customer information in accordance with the Privacy Rules. Priyo respects the privacy of our customers and is committed to treating customer information responsibly. We are dedicated to protecting confidential information and have established standards and procedures to safeguard that personal information.

Responsibilities

Chief Compliance Officer

The CCO, or designee (individually and collectively, referred to herein as Compliance) will report directly to the executive team and is responsible for owning, maintaining and enforcing this Policy. Compliance institutes proper controls that ensure the requirements of this Policy are followed, and identifies and ensures Company managers and employees who are affected by this policy are made aware of its requirements. Compliance also ensures all appropriate personnel have access to resources necessary to comply with this Policy.

Key Definitions

A. Child. An individual under the age of 13.

B. Consumer. An individual who obtains from us a financial product or service that is to be used primarily for personal, family, or household purposes. For example, a consumer is an individual who applies for credit (regardless of whether the credit is extended).

C. Customer (GLBA). A consumer who has a continuing relationship with us under which we provide one or more financial products or services.

   NOTE: A consumer has a more temporary relationship with us than a customer. All customers are consumers, but all consumers are not customers.

D. Personally identifiable financial information. Any information – financial or otherwise – that we have about our customers, which can be tied to a specific customer.

E. Nonpublic personal information. The nonpublic portion of personally identifiable financial information, including any customer lists. Nonpublic personal information consists of nonpublic information that is collected in connection with providing a financial product or service. Specifically, it means:
   - Personally identifiable financial information, which includes:
     - Information a customer provides on an application;
     - Account balance information, payment history, overdraft history and credit or debit card purchase information;
     - Any information collected through an Internet “cookie”;
     - Information from a consumer report;
     - The fact that an individual is or has been one of our customers or has obtained a financial product or service from us; and
     - Any information about our customer if it is disclosed in a manner that indicates that the individual is or has been our customer.
   - Any list, description, or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available. Lists include, but are not limited to, any list of individuals’ names and addresses that is derived in whole or in part using personally identifiable information that is not publicly available, such as account numbers.

     NOTE: Nonpublic personal information does not include information that is available from public sources, such as telephone directories or government records. It also does not include aggregate information or blind data that does not contain personal identifiers.

F. Affiliate. Any company that controls, is controlled by, or is under common control with another company.

G. Nonaffiliated Third Party. Persons or entities *except* affiliates and persons jointly employed by a financial institution and a nonaffiliated third party. GLBA Privacy Rules restrict information sharing with nonaffiliated third parties.

H. Affirmative Consent. As it relates to commercial electronic mail ("email") messages, the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative. If the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's email address could be transferred to such other party for the purpose of initiating commercial email messages.

I. Commercial email message. Any email message the primary purpose of which is to advertise or promote for a commercial purpose, a commercial product or service including content on the Internet. An email message would not be considered to be a commercial email message solely because such a message includes a reference to a commercial entity that serves to identify the sender or a reference or link to an Internet website operated for a commercial purpose.

J. Harvesting. Obtaining email addresses using an automated means from an Internet website or proprietary online service operated by another person, where such service/person, at the time the address was obtained, had provided a notice stating that the operator of such Web site or online service would not give, sell, or otherwise transfer electronic addresses.

K. Hijacking. The use of automated means to register for multiple email accounts or online user accounts from which to transmit, or enable another person to transmit, a commercial email message that is unlawful.

L. Primary Purpose. The primary purpose of an email messages will be deemed to be commercial if it:

1. Contains only the commercial advertisement or promotion of a commercial product or service;
2. Contains both commercial content and "transactional or relationship" content if either:
    a) A recipient reasonably interpreting the subject line of the email message would likely conclude that the message contains commercial content; or
    b) The email message's "transactional or relationship" content does not appear in whole or substantial part at the beginning of the body of the message.
3. Contains both commercial content as well as content that is not transactional or relationship content if a recipient reasonably interpreting either:
    a) The subject line of the email message would likely conclude that the message contains commercial content; or
    b) The body of the message would likely conclude that the primary purpose of the message is commercial.

M. Recipient. An authorized user of the email address to which the message was sent or delivered.

N. Sender. A person who initiates an email message and whose product, service, or Internet website is advertised or promoted by the message.

O. Transactional or Relationship email message. An email message with the primary purpose of facilitating, completing or confirming a commercial transaction that the recipient had previously agreed to enter into; to provide warranty, product recall, or safety/security information; or subscription, membership, account, loan, or other information relating to an ongoing purchase or use.

GLBA Policy Requirements

Information about customers is accumulated at the point of purchase or service, when customer service inquiries are made, or when Priyo responds to customer requests for information.

Information Priyo is Allowed to Share

The law allows Priyo to share information with our affiliates, to the extent that there is a need for our affiliate to have that information, and subject to the opt-out provisions for affiliate marketing and consumer credit report information established by the Fair Credit Reporting Act.

We may share information with other parties, without meeting the “opt-out” condition (defined below), under any of the following conditions:

- To market Priyo’s own financial products or services;
- Where third parties are performing services or functions on behalf of Priyo, including marketing Priyo’s own products or services or products and services offered pursuant to a joint agreement between Priyo and another financial institution, provided that Priyo:
    - discloses that arrangement, and
    - enters into an agreement with the third party to maintain the confidentiality of the information.
- The customer consents;
- It is necessary to effect, administer, or enforce a transaction requested or authorized by the customer;
- To process and service transactions the customer requests or authorizes;
- To protect against potential fraud or unauthorized transactions;
- To protect the confidentiality or security of Priyo’s records;
- For risk control purposes or for resolving customer disputes;
- To persons holding a legal or beneficial interest relating to the customer;
- To persons acting in a fiduciary capacity on behalf of the customer;
- To law enforcement agencies if permitted or required under other provisions of law;
- To respond to judicial process, attorneys, accountants and auditors;

- To respond to governmental authorities for examination, compliance, or other lawful purposes;
- To a consumer reporting agency in accordance with the Fair Credit Reporting Act; or
- To comply with federal state or local laws.

Opt Out Provision

Although Priyo does not currently engage in this practice, if the company does eventually share nonpublic personal information with nonaffiliated third parties in any other capacity than as defined above, Priyo will offer customers the opportunity to “opt out” of the information sharing process. Prior to any such sharing, Priyo will ensure that the customer is provided with the right to opt-out or limit the sharing by notifying Priyo of the intent to “opt out” through the use of a mail-in form or other permissible means. Priyo will share information with its affiliates, and will provide opt-outs as required by FCRA.

GLBA Notice to New Customers

Priyo is required to provide a copy of the GLBA Notice when it enters into a customer relationship with a consumer. A customer relationship means a continuing relationship between a consumer and Priyo, and is established when we provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. Priyo will make the GLBA Notice available on the website and require the consumer/customer to acknowledge receipt of the notice as a necessary step to opening an account with Priyo.

Priyo will provide a clear and conspicuous notice that accurately reflects the privacy policies and practices as they relate to: a) the Company’s customers and b) consumers who may inquire or apply for our services, but do not become customers. This Privacy Notice will be given to the individual when that individual enters into a continuing relationship with the Company. If our sharing of information changes, a new Privacy Notice will be delivered to covered customers. The Privacy notice will inform the customer of the following information:

- Categories of nonpublic personal information we collect;
- Categories of nonpublic personal information we disclose;
- Categories of affiliates and nonaffiliated third parties to whom we disclose nonpublic personal information;
- Categories of nonpublic personal information about our former customers that the bank discloses and the categories of affiliates and nonaffiliated third parties to whom we disclose nonpublic personal information about our former customers;
- An explanation of the consumer’s right to opt-out of the disclosure of nonpublic personal information to nonaffiliated third parties and the ability to opt-out of disclosures of information among affiliates;

- Our policies and practices with respect to protecting the confidentiality and security of nonpublic personal information;
- Any exceptions to the opt-out requirements
-

Priyo does not disclose nonpublic personal information about customers to anyone, except as permitted by law. When customers close accounts or become inactive customers, we adhere to the privacy policies and practices as described in our privacy disclosures. It is our policy not to reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties for their independent use, except as permitted by law.

Annual GLBA Notice

Not less than annually thereafter, Priyo provides a GLBA Notice to applicable customers as long as there is a continuation of the customer relationship. Annually means at least once in any period of 12 consecutive months during which that relationship exists. Priyo will post the GLBA Notice on the website and will send an e-mail to all applicable customers notifying them of the location of the Notice.

Changes to the GLBA Notice

Priyo will not disclose any nonpublic personal information about a customer other than as described in the GLBA Notice, unless Priyo provides a clear and conspicuous revised notice that accurately describes the new policies and practices – along with any appropriate opt-out. In such circumstances, Priyo will not engage in such sharing until after it provides at least 30 days for the customer to opt-out.

Other Information Use and Sharing Restrictions

Account numbers or similar forms of access numbers or access codes for a customer's account cannot be disclosed to any non-affiliated third party for the purpose of marketing non-bank products.

Customer information or other types of information obtained from companies for which Priyo is a service provider may not be used beyond the purpose of the contract.

Business Lines are responsible for ensuring information passed to non-affiliated third parties (e.g.,service providers, marketing companies, etc.) is limited to information needed to fulfill the service provided by the third party.

Non-public personal information obtained concerning non-customers, consumers, and customers may not be disclosed to third parties to make their own product.

Confidentiality and Security

The Company is committed to the security of customer financial and personal information. All of our operational and data processing systems are in a secure environment that protects account information from being accessed by third parties. We maintain and grant access to customer information only in accordance with our internal security standards.

Our employee access to personally identifiable customer information is limited to those with a business reason to know such information. Employees are educated on the importance of maintaining the confidentiality of customer information and on these privacy principles. Because of the importance of these issues, our employees are responsible for maintaining the confidentiality of customer information and employees who violate these privacy policies will be subject to disciplinary measures, including, but not limited to termination.

Maintenance of Accurate Information

The Company continually strives to maintain complete and accurate information about customer accounts.

Maintaining Customer Privacy in Third Party Relationships

When the Company conducts business with third parties, we require vendors and suppliers to maintain similar standards of conduct regarding the privacy of personally identifiable customer information provided to them.

RFPA Policy Requirements

Access to Financial Records by Federal Government Authorities

Before Priyo staff provides a customer's financial records to a federal government authority, one of the following must have been received:

- Voluntarily signed and dated authorization by a customer which –
    - Authorizes such disclosure for a period not to exceed three (3) months;
    - States that the customer may revoke such authorization at any time before the financial records are disclosed;
    - Identifies the financial records authorized to be disclosed;
    - Specifies the purposes for which, and the government authority to which, such records may be disclosed; and
    - States the member's rights under the Act.
- An administrative subpoena or summons. Priyo may release a customer's financial information only if:
    - Priyo has reason to believe the records sought are related to a legitimate law enforcement inquiry;

    - The customer has been served with a copy of the subpoena on or before the date that Priyo is served, and Priyo receives a copy of the notice sent to the customer specifically describing the nature of the inquiry; and
    - Priyo waits ten (10) days from the date the customer was served (or 14 days if the customer was served by mail), to see if notice is received that the customer has filed a motion to stop the subpoena. Priyo will ensure that all required elements are met before disclosing financial information to the federal authority.
- A search warrant.
- A judicial subpoena. If the customer does not challenge the subpoena in court, the records may be available to a federal government authority upon expiration of ten (10) days from the date of service by the court (or 14 days if the notice was mailed to the customer). Priyo will ensure that all required elements are met before disclosing financial information to the federal authority.
- A formal written request by a federal government authority, which is only used when no other authority is available to the federal authority (above). If the customer does not challenge this written request in court, the records may be available to a federal government authority upon expiration of ten (10) days from the date of service by the court (or 14 days if the notice was mailed to the customer). Priyo will ensure that all required elements are met before disclosing financial information to the federal authority.

In addition to one of the above documents, Priyo must also receive a written certification from the federal government authority that the authority has complied with the applicable provisions of the Act. Upon receipt, Priyo will begin to prepare delivery of the requested financial information.

Delayed Notice

Priyo may be required to delay notice to the customer that records have been requested or obtained for ninety (90) days, or indefinitely, if a judge finds that:

- The investigation being conducted is within the lawful jurisdiction of the federal government authority seeking the financial records;
- There is reason to believe the records sought are relevant to a legitimate law enforcement inquiry; and
- There is reason to believe such notice will result in –
    - Endangering the life or physical safety of any person;
    - Flight from prosecution;
    - Destruction of or tampering with evidence;
    - Intimidation of potential witnesses; or
    - Otherwise seriously jeopardizing an investigation or official proceeding or unduly delaying a trial or ongoing proceeding to the same extent as the circumstances above.

Exceptions

The Act's notification and certification requirements do not apply to the following situations:

- When the request for disclosure is not identified with a particular customer, which also includes records or information that is not identifiable as being derived from the financial records of a particular customer.
- When the request for disclosure is pursuant to the exercise of supervisory, regulatory or monetary functions with respect to financial institutions (e.g., examinations, conservatorships and receiverships).
- When the disclosure is pursuant to procedures authorized by the Internal Revenue Code.
- When the disclosure is pursuant to the filing of a Suspicious Activity Report (SAR) when Priyo believes that information may be relevant to a possible violation of a statute or regulation.
- When the disclosure is required, pursuant to a federal statute or regulation.
- When the request for disclosure is sought under the Federal Rules of Civil or Criminal Procedure, or comparable rules of other courts in connection with litigation to which the government authority and the customer are parties.
- When the request is pursuant to an administrative subpoena issued by an administrative law judge in an adjudicatory proceeding.
- When the request is pursuant to legitimate law enforcement inquiries, and the information sought is the name, address, account number and type of account of any customer.
- When the request is pursuant to a grand jury subpoena. In these instances, Priyo staff will not disclose the existence of such a subpoena to the customer, or that financial records were turned over to a grand jury.
- When the records are sought by the General Accounting Office pursuant to an authorized proceeding, investigation, examination or audit directed at a government authority.
- When Priyo or supervisory agency provides any record of any officer or employee to the U.S. Attorney General, a state law enforcement agency, or the Secretary of the Treasury that there is reason to believe there were crimes against Priyo by an insider.

Special Procedures

Access to Financial Records for Certain Intelligence and Protective Purposes

Aside from the exceptions listed above, Priyo may provide records to the following entities:

- A government authority authorized to conduct foreign counter- or foreign positive-intelligence activities, when the authority has certified in writing that it has complied with the applicable provisions of the Act;
- The Secret Service for the purpose of conducting its protective functions, when the agency has certified in writing that it has complied with the applicable provisions of the Act;
- A government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism, when the authority has certified in writing that it has complied with the applicable provisions of the Act; or
- The Federal Bureau of Investigation (FBI), when the FBI Director (or its designee) certifies in writing that such records are sought for foreign counterintelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis protected by the first amendment to the U.S. Constitution.

Priyo staff will not disclose that a government authority listed above has sought or obtained access to financial records when such authority certifies that there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or safety of any person.

Emergency Access to Financial Records

Priyo staff may release financial records to a government authority when the authority determines that delay in obtaining access to such records would result in imminent danger of the following:

- Physical injury to any person;
- Serious property damage; or
- Flight to avoid prosecution.

In these cases, the government authority will submit the required certificate of compliance with the Act, which is signed by a supervisory official of a rank designated by the head of the government authority.

COPPA Policy Requirements

The Company currently does not operate a website or online service directed to children that collects or maintains personal information about them, or knowingly collects or maintains personal information from a child online. In the event that the Company does, Priyo will comply with the requirements of COPPA including:

- Providing notice on the Company's website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information;
- Obtaining verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children;
- Providing a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance;
- Not conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity and
- Establishing and maintaining reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

CCPA

The California Consumer Privacy Act of 2018 ("CCPA") gives consumers more control over the personal information that companies collect about them. The act secures privacy rights for California consumers including:

- The right to know about the personal information a company collects about a consumer and how it is used and shared;
- The right to delete personal information collected from a consumer (with some exceptions);
- The right to opt-out of the sale of a consumer's personal information; and
- The right to non-discrimination for excercising a consumer's CCPA rights.

If a consumer is a California resident, CCPA requires the Company to provide the consumer with certain notices prior to the Company's collection and use of personal information about a consumer. Priyo must provide consumers a notice with information set forth below.

Right to Know About Personal Information Collected, Disclosed, or Sold

- Explanation that a consumer has the right to request that the Company disclose what personal information it collects, uses, discloses, and sells;
- Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the Company;
- General description of the process the Company will use to verify the consumer request, including any information the consumer must provide;
- Identification of the categories of personal information the Company has collected about consumers in the preceding 12 months.
- Identification of the categories of sources from which the personal information is collected;
- Identification of the business or commercial purpose for collecting or selling personal information; and
- Disclosure or Sale of Personal Information which includes
    - Identification of the categories of personal information, if any, that the Company has disclosed for a business purpose or sold to third parties in the preceding 12 months.
    - For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.
    - Statement regarding whether the Company has actual knowledge that it sells the personal information of consumers under 16 years of age.

Right to Request Deletion of Personal Information

- Explanation that the consumer has a right to request the deletion of their personal information collected by the Company;
- Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the Company; and
- General description of the process the Company will use to verify the consumer request, including any information the consumer must provide.

Right to Opt-Out of the Sale of Personal Information

- Explanation that the consumer has a right to opt-out of the sale of their personal information by a Company; and
- Statement regarding whether or not the Company sells personal information and the contents of the notice of right to opt-out.

Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights

- Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

Other Information

- Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf;
- A contact for questions or concerns about the Priyo's privacy policies and practices; and
- Date the privacy policy was last updated.

Monitoring and Testing

Priyo will ensure that compliance with Privacy requirements is independently monitored and tested at least annually. Results from the testing are maintained and reported to the Board.

CAN-SPAM Policy Requirements

The CAN-SPAM Act details several prohibitions related to the sending of commercial email messages. Priyo has established internal procedures to identify an email message where the primary purpose would be considered commercial under CAN-SPAM to comply with the following requirements:

- Don't use false or misleading header information. The "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
- Don't use deceptive subject lines. The subject line must accurately reflect the content of the message.
- Identify the message as an ad. The fact that the message is an advertisement must be clearly and conspicuously disclosed.
- Tell recipients where Priyo is located. The message must include a valid physical postal address. This can be Priyo's current street address, a post office box registered with the U.S. Postal Service, or a private mailbox registered with a commercial mail receiving agency established under Postal Service regulations.
- Tell recipients how to opt out of receiving future email. The message must include a clear and conspicuous explanation of how the recipient can opt out of receiving future emails. Any notice containing the explanation of how the recipient can opt out should be

designated, so that it is easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. A return email address or another easy Internet-based way to allow people to communicate their choice to opt out of further email communications must be provided. A menu can be used to allow a recipient to opt out of certain types of messages, but the option to stop all commercial messages must also be included. Make sure that Priyo's spam filter doesn't block these opt-out requests.

- Honor opt-out requests promptly. Any opt-out mechanism offered must be able to process opt-out requests for at least 30 days after a message is sent. A recipient's opt-out request must be honored within 10 business days of receipt. Priyo cannot charge a fee, require the recipient to provide any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once Priyo has been notified of an opt-out request from the email recipient, Priyo is prohibited from selling or transferring the recipient's email address to any other party, even in the form of a mailing list. The only exception is that the address may be transferred to a company hired to help ensure compliance with the CAN-SPAM Act.
- Third-party monitoring. The law makes it clear that even if a third party is hired to handle Priyo's email marketing campaigns or solicitations, both Priyo and the third-party vendor that distributes the message may be held legally responsible and/or liable for violations of the CAN-SPAM Act. Any email marketing materials or solicitations created through a third-party vendor relationship are to be reviewed for compliance with the CAN-SPAM Act and this policy prior to distribution.

Training

The Company will train all employees on Privacy and CAN-SPAM Compliance each calendar year, and monitor and track completion of this training. Other periodic or ad hoc trainings may be added as required.

Record Retention

Federal privacy requirements do not specifically require Priyo to maintain records for a specified time period. All records related to compliance with the Privacy laws for any Priyo account must be maintained in accordance with the Company's record retention policies and practices. The CCPA requires the Company to document consumer requests and the Company's responses to those requests for a minimum of two years.

Priyo must also keep a record of all marketing and advertising materials consistent with all applicable laws and in accordance with its record retention practices. All documentation supporting the review and approval of materials related to marketing and advertising also must be maintained.