

# Respect and Protect: Our Privacy Mission

Guidelines for Privacy

June 2009



# Contents

Introduction .....	1
How Do We Give Notice? .....	2
Personally Identifiable Information — PII .....	2
Notice .....	2
How Do We Manage and Use PII? .....	4
Managing PII .....	4
Customer Choice: Primary Use Versus Secondary Use ..	4
Security and Protection of PII .....	5
How Do We Share PII? .....	7
Internal Disclosures .....	7
External Disclosures .....	7
Supplier Policy — Contract Clause .....	7
Accountings of Disclosures .....	8
How Do We Provide Access and Redress? .....	9
Requesting Access .....	9
Responding to Access Requests .....	9
Responding to Amendment Requests .....	9
Redress: Complaints and Inquiries .....	10
Special Rules .....	11
Direct Marketing to Employees .....	11
E-Mail Marketing .....	11
Federal Laws and Guidelines .....	13
Federal Laws — Required Compliance .....	13
Federal Laws — Voluntary Compliance .....	13
Federal Agency Guidelines .....	14



# Introduction

For over 200 years, the Postal Service has had a unique mission—providing affordable universal mail service to everyone in America—no matter who, no matter where. Throughout our history, our job was simply to deliver the mail while safeguarding its cover and contents. We have done that job very well...building a brand that is one of the most trusted.

To meet the demands of today's fast-paced world with its focus on convenience, we offer products and services that make it necessary to collect and store personal information each day. This has expanded our mission to include the proper collection, use, and protection of customer and employee information. It is our responsibility to respect and protect the privacy and security of the personal information we maintain. This responsibility applies to every one of us, at every level.

Why? Our continued success depends on protecting personal information. It also supports our Strategic Transformation Plan by promoting growth through added value to customers and improving the workplace environment.

Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*, provides guidance for Postal Service employees, suppliers, and other authorized users with access to Postal Service records and information resources. The handbook also helps customers, employees, suppliers, and others understand how their information is collected, used, disclosed, and safeguarded.

Handbook AS-353 is available on the Postal Service Intranet:

- Go to <http://blue.usps.gov/cpim/>
- Click *HBKs*.
- Click *Guide to Privacy, the Freedom of Information Act, and Records Management*.

If you have questions about our privacy policies and procedures:

- Visit the Privacy website at <http://blue.usps.gov/caweb/privacy/welcome.htm>;
- E-mail us at [USPSEmployees@usps.gov](mailto:USPSEmployees@usps.gov); or
- Write to us at:

PRIVACY OFFICE  
US POSTAL SERVICE  
475 LENFANT PLZ SW RM 10407  
WASHINGTON DC 20260-2200

# How Do We Give Notice?

## Personally Identifiable Information – PII

Just like you, every customer and employee shares information about themselves—like name and address—in work, personal, and business settings. Some information is common: many people are named John or Sally. Some information is unique, like a Social Security or employee identification number. Information that allows a person to be identified, contacted, or located is called Personally Identifiable Information or PII.

## Notice

Whenever we collect PII, we give Notice to let our customers and employees know we need their PII and we intend to protect it. Follow rules 1 through 4 below about how to provide Notice when collecting information from individuals (customers or employees) or business customers.

Any Postal Service channel (e.g., online, forms, or PostalEase) that collects PII about individuals, and which retrieves that information by name or other personal identifier, must have a Privacy Act notice. The Privacy Act notice contains four components; each is described below and identified by number in exhibit 1.

1. The purpose for which the information is collected.
2. The laws that allow us to collect the information.
3. Whether or not providing the information is voluntary, and the consequences if the information is not provided.
4. The circumstances (Routine Uses) in which the information may be disclosed.

### Exhibit 1: Sample Privacy Act Notice

**Privacy Act statement:** <sup>①</sup> Your information will be used to provide you requested products, services, or information. <sup>②</sup> Collection is authorized by 39 USC 401, 403, and 404.

<sup>③</sup> **Providing the information is voluntary, but if not provided, we may not process your transaction.** We do not disclose your information without your consent to third parties, except to facilitate the transaction, to act on your behalf or request, or as legally required. This includes the following limited circumstances: to a congressional office on your behalf; to financial entities regarding financial transaction issues; to a USPS auditor; to entities, including law enforcement, as required by law or in legal proceedings; and to contractors and other entities aiding us to fulfill the service (service providers). For more information on our privacy policies see our privacy link on *usps.com*. <sup>④</sup>

Information from business customers is covered by Postal Service privacy policies, not the Privacy Act. When we collect information from business customers, we provide a simple notice that directs them to *usps.com* to learn more about our privacy policies.

The Privacy Office is responsible for reviewing and approving all notices that collect PII via each channel. These include online and hardcopy forms, web applications, telephone scripts, and in-person communications.

## PRIVACY ESSENTIALS

### DO:

- Make sure a notice is provided whenever personal information is collected.
- Be sure that the Privacy Office has reviewed and approved the notice.

### DON'T:

- Forget to provide a notice whenever you are collecting personal information regardless of how it's collected (e.g., phone, form, in person, online).

## How Do We Manage and Use PII?

We have made a strong commitment to privacy supported by a written policy that meets or exceeds government regulations and private sector best practices. Our privacy policy is very important to us, to our employees, and to our customers. Our policy is a promise about the information we collect, how we use it, who we share it with, what choices we offer, and how we protect it.

### Managing PII

As outlined in Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*, we cannot begin to collect or manage PII without determining if a Privacy Act system of records (SOR) is required and, if so, making sure there is an authorized SOR that governs how to manage the PII.

What's an SOR? Simply put, it is a published document that describes requirements for how to manage PII.

When is it needed? It is needed if a database, file, or program maintains PII and information is retrieved from it by name or some other personal identifier.

For example, since information from the National Change of Address system (NCOA) is retrieved by customer name, it has an SOR, "Address Change, Mail Forwarding, and Related Services," which outlines requirements for NCOA data (e.g., storage, safeguards, retention, sharing, and disposal). All SORs may be found in the Appendix of Handbook AS-353.

The Privacy Office is responsible for creating, amending or deleting an SOR, as necessary, using an established protocol, which includes publishing a notice in the *Federal Register* for public comment.

### Customer Choice: Primary Use Versus Secondary Use

Primary use of PII occurs when we use customers' personal information to provide a requested product or service, such as Click-N-Ship® or The Postal Store®.

Secondary use occurs when we want to use this information for another purpose—such as to market a different product or service or share it with our partners. Customers must have a choice about these secondary uses. Consumers must be given the opportunity to actively opt in (see exhibit 2). For businesses, we use an opt-out standard, assuming that they want to hear from us or our partners unless they tell us otherwise.



## Security and Protection of PII

Information about customers, employees, or other individuals must be protected in accordance with Handbook AS-805, *Information Security*. Common sense plays a big role in protecting PII.

For example:

- Be aware of your surroundings when discussing PII.
- Minimize the inclusion of PII in communications.
- Send PII only to those who need it for business purposes.
- Encrypt files that contain PII.
- Secure sensitive documents (e.g., leave slips and pay adjustments) in locked cabinets.

When traveling:

- Keep removable media such as laptops, flash drives, BlackBerrys, and CDs with you at all times or locked in a safe place.
- Use a portable locking device or cable lock to secure your laptop both inside and outside the office.

## PRIVACY ESSENTIALS

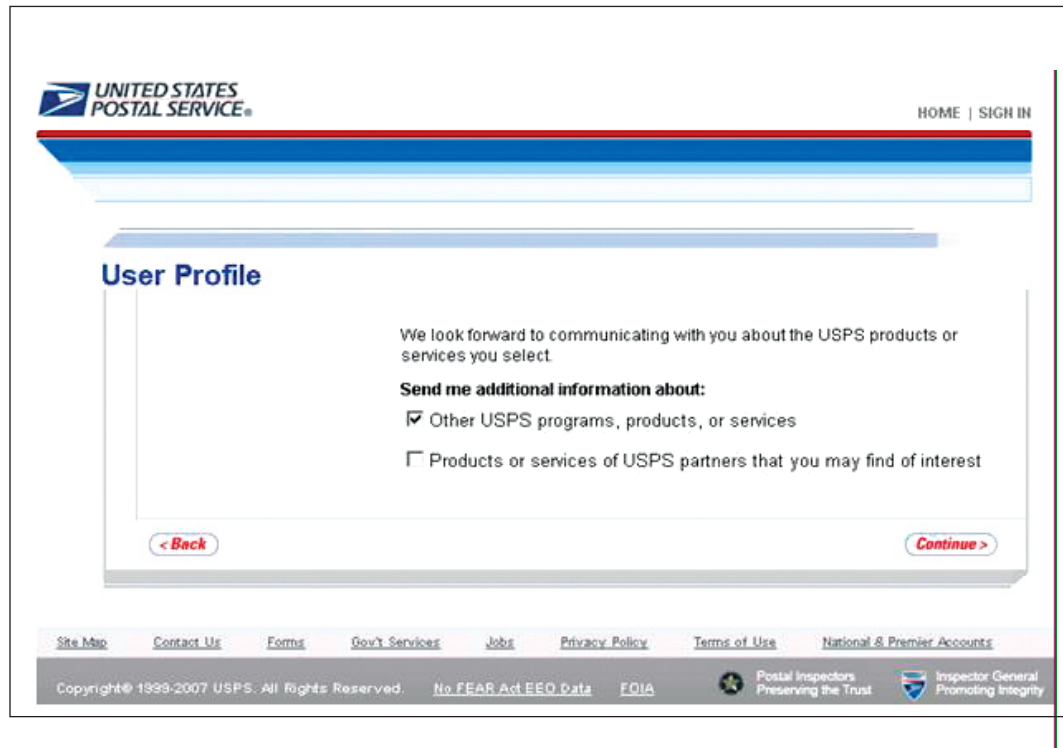
### DO:

- Review the Appendix in Handbook AS-353 for a list of authorized systems of records and how to manage data.
- Notify the Privacy Office if a system of records needs to be created, amended, or deleted.
- Secure and protect PII.

### DON'T:

- Collect PII unless an authorized system of records is established.
- Use PII for secondary purposes without appropriate customer consent.

## Exhibit 2: Sample Opt-in Screen (Secondary Use)



The screenshot shows the USPS website's 'User Profile' section. At the top left is the USPS logo, and at the top right are links for 'HOME' and 'SIGN IN'. Below a blue and red header bar, the 'User Profile' title is displayed. The main content area contains a message: 'We look forward to communicating with you about the USPS products or services you select.' Below this is a section titled 'Send me additional information about:' with two radio button options: 'Other USPS programs, products, or services' (which is selected) and 'Products or services of USPS partners that you may find of interest'. At the bottom of the form are two buttons: '< Back' and 'Continue >'. The footer contains a navigation menu with links for 'Site Map', 'Contact Us', 'Forms', 'Gov't Services', 'Jobs', 'Privacy Policy', 'Terms of Use', and 'National & Premier Accounts'. Below the navigation menu is a copyright notice: 'Copyright © 1999-2007 USPS. All Rights Reserved.' followed by links for 'No FEAR Act EEO Data' and 'FOIA'. On the right side of the footer are two logos: 'Postal Inspectors Preserving the Trust' and 'Inspector General Promoting Integrity'.

UNITED STATES  
POSTAL SERVICE®

HOME | SIGN IN

### User Profile

We look forward to communicating with you about the USPS products or services you select.

**Send me additional information about:**

Other USPS programs, products, or services

Products or services of USPS partners that you may find of interest

[< Back](#) [Continue >](#)

[Site Map](#) [Contact Us](#) [Forms](#) [Gov't Services](#) [Jobs](#) [Privacy Policy](#) [Terms of Use](#) [National & Premier Accounts](#)

Copyright © 1999-2007 USPS. All Rights Reserved. [No FEAR Act EEO Data](#) [FOIA](#)

Postal Inspectors  
Preserving the Trust

Inspector General  
Promoting Integrity

## How Do We Share PII?

The Postal Service has strict limitations on how personal information can be disclosed, whether it is inside or outside the Postal Service.

### Internal Disclosures

Information may be disclosed to employees — or employees of a supplier fulfilling a Postal Service function — who need the information to perform their jobs. This situation provides an example of official need-to-know.

### External Disclosures

External disclosures may only be made under very limited conditions. Key examples include:

1. **Consent** — the individual about whom information is being disclosed authorizes the disclosure in writing.
2. **Routine Use** — the disclosure is listed in the privacy notice and applicable system of records.
3. **Publicly Available Information** — information such as employment data (name, job title, grade, current salary, duty status and dates of employment) and business change-of-address.

### Supplier Policy — Contract Clause

We often contract with suppliers and partners to assist us in our work with employees and customers. Any time we share personal information with suppliers and partners, we have to be careful to specify the privacy practices they must follow to protect that information. Those practices have to be at least as robust and thoughtful as our own. To accomplish this, we require specific contract language with these suppliers. Consult *USPS Supplying Principles and Practices*, Clause 1-1, Privacy Protection, for details:

- Go to: <http://blue.usps.gov/policy/>.
- In the left-hand frame, click *Clauses & Provisions*.
- Scroll down and click *Clause 1-1*.

## Accountings of Disclosures

When we release information contained in a system of records to a party outside the Postal Service, the custodian of the record must keep an accurate accounting of the disclosure. For example, if information from a change-of-address order is released to a process server, the following information must be documented: the date, nature, purpose, and to whom (name and address of the agency or person) the disclosure was made.

Why? Because the Privacy Act requires us to be able to respond accurately and intelligently to individuals' requests about how we disclosed information about them. We must keep records of these disclosures for at least 5 years, or the life of the record, whichever is longer.

Accountings of disclosures are not required for : (1) internal disclosures; (2) disclosures of information that is publicly available; or (3) disclosures to individuals about themselves.

## PRIVACY ESSENTIALS

### DO:

- Disclose information internally if there is an official need-to-know.
- Maintain records about any disclosures made from a system of records as required by the Privacy Act.
- Include the Privacy Protection Contract Clause in all contracts with suppliers that will have access to PII.

### DON'T:

- Release any information unless specific conditions are met.

# How Do We Provide Access and Redress?

## Requesting Access

Employees and customers who have provided personal information to the Postal Service may request to review the information we maintain about them in a Privacy Act system of records (SOR). The “Notification Procedures” and “Records Access Procedures” located in each SOR will tell you how and where to direct the request.

You can direct employees or customers to the program manager, the office that handled any prior complaint or inquiry, or the Privacy Office for assistance.

## Responding to Access Requests

Here’s what to do if you receive a request: First, review the request to determine if it provides enough information to allow you to identify and locate the record. If not, then seek clarification from the requester. Refer misdirected requests to the appropriate office. If you are not sure which office is appropriate, forward the request to:

MANAGER  
RECORDS OFFICE  
US POSTAL SERVICE,  
475 LENFANT PLZ SW RM 5821  
WASHINGTON DC 20260

Notify the requester that you have referred the request to the appropriate office.

You must acknowledge a request within 10 business days. If the requested records are not immediately available, then give the requester a date of availability. Inform the requester if the records have been destroyed or cannot be located.

Once the records are located and a determination of release has been made, you may provide them to the requester in writing or in person. Be sure to document that access — in writing or in person — was granted.

## Responding to Amendment Requests

If employees or customers believe that information about them is not accurate, relevant, timely, or complete, they may request that the information be amended. If an amendment is requested, you have 10 business days to provide written acknowledgment of the request. You must:

- Make the correction promptly and notify the requester of the revision; or
- Inform the requester of the decision to keep the record “as is,” provide the reason for the decision, and tell the requester how he or she may appeal to the General Counsel.

Customers registered with *usps.com* may log in to their accounts to update their information and amend their profile to reflect their preferences.

## Redress: Complaints and Inquiries

The Privacy Office is available to help employees and customers who have questions or complaints about our privacy policy and how we use their information.

## PRIVACY ESSENTIALS

### DO:

- Remember that employees and customers have a right to request access to the information we maintain about them.
- Make sure the requester provides enough information to identify and locate the records being sought.
- Acknowledge requests for access or amendments within 10 business days.
- Respond to complaints and inquiries from employees and customers, or direct them to the Privacy Office.

### DON'T:

- Deny a request to amend records without providing the reason and appeal procedures.

## Special Rules

The Postal Service is one of the most trusted of all federal agencies and it touches almost everyone in America almost every day. Realizing that there are many instances for which we collect PII, the Postal Service has established the following management instructions to set forth additional privacy protections for certain programs:

### Direct Marketing to Employees

Growing revenue is a critical strategy for the Postal Service. The management instruction (MI) AS-333-2004-7, *Direct Marketing Co-branded Products or Services to Employees*, outlines the policies and procedures by which the Postal Service may enter into agreements with businesses to market co-branded products to our employees by sending direct mail to their homes. These agreements provide value to employees, the Postal Service, and the business firm through the offer of quality products at competitive prices, revenue sharing or other benefits to the parties, and the business's use of direct mail.

*Does this mean the Postal Service is giving employee names and mailing addresses to these business firms?* Absolutely not! The business firm never receives access to the list. The employee mailing list may be provided to a third-party mailing house under strict contract controls and nondisclosure agreements. If an employee responds to a co-branded offer, then that employee becomes a customer of the business firm, which may obtain personal information directly from the individual.

Employees who have questions about this program or their privacy may contact the Privacy Office.

MI AS-333-2004-7 is available on the Postal Service Intranet:

- Go to <http://blue.usps.gov/cpim/>.
- Click *MI*s.
- Click *Direct Marketing Co-branded Products or Services to Employees*.

### E-Mail Marketing

We have to keep in mind that our customers have choices about what we send them. The Postal Service outlines its policies and procedures for e-mail marketing in MI AS-350-2004-4, *Marketing E-mail*. This policy applies when the Postal Service or its supplier sends an e-mail message that markets a product or service different from what the customer registered for with the Postal Service.

Postal Service requirements for marketing by e-mail include the following:

- The e-mail may be sent only to consumers who have opted-in or businesses that have not opted-out.
- All marketing e-mail must accurately identify the sender and contain headers showing the e-mail source.
- The subject line must not be misleading about the content of the message.
- The body of the message must include information about how customers can cancel further e-mails from the Postal Service.
- Cancellation requests from any verified source must be honored within 10 days.

For specific procedures, consult MI AS-350-2004-4:

- Go to <http://blue.usps.gov/cpim/>.
- Click *MI*s.
- Click *Marketing E-mail*.



## Federal Laws and Guidelines

Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*, describes the Postal Service's policies and procedures about information privacy as they relate to customers or employees. The Privacy Office has developed its privacy policy and procedures to reflect the best business models and practices of the public and private sectors.

The Postal Service complies with the following laws and guidelines:

### Federal Laws – Required Compliance

**Postal Reorganization Act** — restricts the Postal Service from sharing customer or mailing lists to the public by any means or for any purpose, except as specifically provided by law.

**Privacy Act of 1974** — applies to federal agencies, including the Postal Service. The Act provides privacy protections for personal information that agencies maintain in a system of records. A system of records is a file, database, or program from which information is retrieved by name or other personal identifier.

**Freedom of Information Act** — gives the public access to records maintained by the Postal Service, unless the records are exempt from disclosure.

### Federal Laws – Voluntary Compliance

**Gramm-Leach-Bliley Act** — governs the treatment of personal information when certain financial services are provided in the private sector; requires that customers be given notice about data practices and choices as to whether data can be shared with unaffiliated parties.

**CAN-SPAM Act** — establishes requirements for those who send commercial e-mail, and gives consumers the right to ask e-mailers to stop e-mailing them.

**eGovernment Act of 2002** — requires agencies to establish certain online privacy policies and conduct Privacy Impact Assessments — equivalent to a Postal Service Business Impact Assessment (BIA) — when systems collect or manage PII. The BIA is a document that addresses all privacy and security requirements, including ensuring privacy compliance, determining the sensitivity and criticality of a system, and developing the appropriate security plan.

## Federal Agency Guidelines

***Privacy Principles of the Federal Trade Commission*** establish fair information principles that it recommends the private sector provide to its customers. The principles are notice, choice, access, security, and redress.

***Privacy Guidelines of the Office of Management and Budget (OMB)*** emphasize the Privacy Act and online privacy policies. OMB gives particular attention to certain technologies on agency web sites, including web analyses tools such as cookies, and requires notice and agency head approval for their use.



