Federal Trade Commission
Privacy Impact Assessment

Off-site Mailroom Digitization (BrightKey)

February 2025

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission receives thousands of pieces of hardcopy mail on a daily basis that it must sort, categorize, and deliver in a timely manner to the intended recipients at the FTC. Previously, security screening for all DC-area FTC staff (which includes employees and contractors) was conducted at FTC headquarters; once screened, the hardcopy mailings were distributed to staff through pre-designated mailstops located throughout FTC's two main facilities. The inherent risk of screening and sorting mail onsite prompted the Commission to reevaluate safety measures and consider outsourcing mail screening and processing services to a third-party vendor. Thus, the FTC's Offsite Mailroom Digitization was developed to reduce security risks associated with reception of physical mail and any harmful materials that may potentially be included (explosives, chemicals, etc.). The FTC Office of the Chief Administrative Services Officer (OCASO) contracted with BrightKey, a federally approved and vetted vendor, to scan and digitize all incoming mail and electronically distribute the mail to FTC staff at the Washington, DC locations. As part of the operational shift to offsite mail screening and digitization, all mailings (USPS, FedEx, UPS, DHL, etc.) sent to DC-area FTC facilities undergo offsite security screening and digitization through BrightKey.

Digitized mailings are emailed directly from BrightKey to DC-area FTC staff via their FTC.gov email account. The exception to this is mail that is considered Classified (Confidential, Secret, or Top Secret); such items are not digitized and are instead hand delivered to the authorized FTC employees. Additionally, the FTC Human Capital Management Office (HCMO) receives all its mail in hardcopy form due to the sensitivity of the mail they typically receive.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The information in this system is collected, maintained and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58 and other laws and regulations the Commission enforces.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☐ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: See Note Below
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

Note: The data elements indicated in the table above are collected from the recipients of mail (i.e., FTC employees and contractors). The mail screened and digitized by BrightKey may contain any and all types of data, including potentially sensitive information pertaining to the sender. The FTC, and BrightKey, take all applicable and practical measures to ensure that mail is delivered only to the intended recipient or designee authorized to receive that information.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

As mentioned above, the mail screened and digitized by BrightKey may contain any and all types of data; this may include linkable information that would not otherwise constitute as PII. The FTC, and BrightKey, take all applicable and practical measures to ensure that all PII and sensitive PII are handled in a secure fashion, and that the mail is delivered only to the intended recipient or designee authorized to receive that information.

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.3 What is the purpose for collection of the information listed above?

BrightKey collects all hardcopy mailings postmarked for the Washington, DC FTC Offices for the purpose of screening and digitizing the mail for electronic delivery. The information collection is necessary in order to ensure the mail is delivered to the appropriate FTC staff. After the mail is collected at their offsite facility, BrightKey staff screen the hardcopy mailings by searching for chemical, biological, and explosives. After screening, all paper mailings are digitally scanned and forwarded to the intended FTC staff via encrypted email. BrightKey maintains the digital files for a period of 48 hours, after which time the digital files are wiped from its network and electronic systems.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	***Type of Data Provided & How It Is Collected***
Individual Members of the Public	The FTC receives solicited and unsolicited mailings from members of the public on a daily basis. Such mailings reach the agency through various carriers, both national and international (e.g., USPS, FedEx, DHL, and UPS). Any mail that is not marked Classified is screened for hazardous materials, then digitally scanned for electronic delivery. The mail can contain any and all types of information, including PII and/or sensitive information. BrightKey maintains the digital files for a period of 48 hours, after which time the digital files are wiped from its network and electronic systems.
Private Law Firms/External Counsel	The FTC receives mailings to support litigations and other FTC/consumer interactions. As with all other mail directed to the Washington, DC FTC offices, these mailings are collected through both national and international mail carriers. The mail is digitized, and the information is retained in BrightKey's systems for a period of 48 hours.
Other Federal Agencies	To support the FTC's law enforcement activities, solicit support, and/or share operational information, the FTC often receives correspondence from other agencies across the Federal government. The mail is screened, digitized, and electronically delivered to the intended FTC party.
FTC Employees	On a monthly basis, BrightKey receives from the FTC an email with a comma-separated values (CSV) file containing the list of new FTC employees. This file contains the employee's name, email address, office/bureau, organization code, mail stop location, room location, and desk number. BrightKey uses this information to ensure the new

Source of Data	*Type of Data Provided & How It Is Collected*
	employees' mail are digitized and/or delivered in person accordingly.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
BrightKey	Hardcopy mailings are opened and screened by BrightKey at their offsite facility. Once screened, mailings are digitally scanned by BrightKey and then emailed to the intended FTC recipient. BrightKey maintains the digital files for a period of 48 hours, after which time the digital files are wiped from its network and electronic systems.
FTC employees and contractors	FTC employees and contractors with an ftc.gov email address receive the digitally scanned mailings via email from BrightKey. FTC employees and contractors do not have access to their own information within the BrightKey system.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

BrightKey is an approved and security vetted contractor. The FTC has conducted expansive security assessments of BrightKey's network and associated IT based systems to ensure proper functionality and security of FTC mailings that are digitally sent to FTC staff. Only authorized BrightKey staff have access to the FTC's digitized mail in the BrightKey system. After scanning the hardcopy mail, the digitized mail images are securely emailed to the intended FTC recipient(s). The digitized mail is deleted from BrightKey's systems after approximately 48 hours.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third-party service provider.

BrightKey maintains its own incident response plan, and in the case of a potential loss or breach of FTC data, BrightKey is required to notify the FTC as soon as practicable. BrightKey monitors its systems through program logs, reports, and automated alerts to ensure that no threats or abnormal network activity goes undetected. BrightKey receives alerts and notifications from different services depending on the type of incident or threat. Upon detection of a threat or anomaly, BrightKey triggers its Incident Response Team to

investigate the threat and determine its cause and nature. In the event of a threat or loss of data, the FTC would be notified immediately or as soon as reasonably practicable.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☐ Privacy Act Statement (☐ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): FTC employee information is collected for the purpose of routing digitized mail to them via email. FTC employees are notified about their information collection as part of the hiring and onboarding process.

☒ Notice is not provided (explain): While information pertaining to members of the public is maintained in the BrightKey system in the form of digitized mail received by the FTC, it is not feasible or practical to provide notice to members of the public prior to the information digitization. The information is maintained in BrightKey's systems as part of the scanned image of the mail, not as separate data elements collected directly from the individuals. Thus, notice is provided through this PIA to members of the public; additional information regarding BrightKey's mail processing services is also available in the Sentinel Network Services (SNS) PIA and the General Support System (GSS) PIA.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Members of the public who mail the FTC do not have the opportunity to decline to provide their information to BrightKey as it pertains to the mail digitization process, nor do they have the opportunity to consent to particular uses of their information. It is not feasible or practical to provide notice to members of the public prior to the information digitization. However, as stated above, the information is maintained in BrightKey's systems as part of the scanned image of the mail, not as separate data elements collected directly from the individuals. Additionally, the data is deleted from BrightKey's systems after 48 hours, reducing the risk of maintaining the data longer than necessary.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Only authorized BrightKey staff have access to the data in the BrightKey system. Members of the public and FTC staff do not have access to the digitized FTC mail in the BrightKey system.

An individual may make a request under the Privacy Act for access to information maintained about themselves by FTC and BrightKey. The FTC's privacy policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

The FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the Agency. The FTC's privacy policy provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the Privacy Act for access to information maintained by the FTC and BrightKey. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file requests with the FTC under the FOIA for agency records that may be about them (if they are not exempt from disclosure to them under those laws).[2] Additionally, individuals may contact the FTC with any complaints, questions, or concerns via phone or email available on www.ftc.gov or contact the FTC Chief Privacy Officer directly.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

On a monthly basis, the FTC shares with BrightKey a CSV file containing the names of current FTC employees and contractors. This file is compiled by OCIO and contains the employee's name, email address, office/bureau, room location, desk location, organization code, and mail stop location, if applicable. This file is used by BrightKey to ensure that digitized mail is delivered to the intended and authorized recipients.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

As a safety precaution to protect FTC staff and FTC facilities, BrightKey receives all FTC mail via USPS, FedEx, DHL, and UPS. Mail is processed through multiple screening systems that are designed to detect chemical, biological, radioactive, nuclear, and explosive (CBRNE) agents. Once the mail has been digitized, it is delivered securely to the FTC

[2] 9 See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13 (FTC Privacy Act rules).

recipient via encrypted email. Digitized mail is maintained by the vendor for up to 48 hours, after which it is purged from BrightKey's systems.

On a monthly basis, the FTC provides BrightKey with a list of names and contact information of current employees and contractors, information that is required for the purpose of adequately routing electronic mail to FTC staff. The information is maintained by authorized BrightKey personnel who have been screened and vetted through the FTC Personnel Security Office. BrightKey is not at liberty to disclose any FTC information, including the contents of any mail it handles on behalf of the FTC, to any third-party without prior written approval from the FTC.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable. PII is not used in the course of system testing, training, or research.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

BrightKey maintains the digitized mail for up to 48 hours after it has been imaged, after which the vendor conducts a data sanitization process that involves a single pass over-write from the server, thus making the data unrecoverable.

The digitized mail that is delivered to the FTC employee via encrypted email is maintained in the FTC's General Support System (GSS) and is subject to the FTC's email retention policy (up to seven years), after which it is automatically deleted.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

☒ Not Applicable. The project/system does not employ the use of a website.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	*Mitigation Strategy*
Digital mail may inadvertently be sent to the wrong FTC employee via email.	On a monthly basis, FTC Logistics Branch staff provides the vendor with a CSV file created by OCIO that captures the proper email address for each FTC employees. The CSV file is shared with the vendor as to update their digital mail distribution listings. Vendor staff uses the CSV file to properly address the electronic distribution of mailings to applicable FTC staff.
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	Vendor system administrators strictly manage access control and limit the use and access of all data to purposes for which it was collected. Associated vendor mailroom staff are security screened and vetted through the FTC Personal Security screening process.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

BrightKey maintains a network firewall and antivirus programs to ensure the security and privacy of the data maintained in its systems. This includes the detection of unauthorized wireless access points, unusual network usage, activating authorized users and deactivating unauthorized users as needed.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Not applicable. The BrightKey system is not considered a Privacy Act system of record because information in the system is not retrieved on a routine basis using a unique identifier.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The collection, use, and disclosure of information discussed in this PIA are consistent with the FTC's Privacy Policy. Access logs, storage logs, and firewall logs are periodically reviewed to ensure that users are complying with BrightKey's policies and procedures.

BrightKey ensures that FTC data scanned and emailed remains logically separate from other data on the BrightKey network. Per its contract with the FTC, BrightKey purges the digitized mail data after 48 hours.