Federal Trade Commission
Privacy Impact Assessment

Electronic Document Management System (Documentum)

October 2019

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC, Commission or the agency) is an independent federal government law enforcement and regulatory agency with authority to promote consumer protection and competition through prevention of unfair, deceptive and anticompetitive business practices; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish these missions without unduly burdening legitimate business activity.

The FTC relies on an electronic document management system (EDMS) to support the agency's business. This system allows staff to track, search and access various types of agency documents, such as staff memoranda to the Commission; Commission approved reports; filings and orders in FTC adjudicative proceedings; and filings in federal court cases. Maintaining these documents in an EDMS also facilitates responses to Freedom of Information Act (FOIA) and other disclosure requests by providing search and access capability for responsive documents.

Documentum contains all of the documents and metadata that were in the system that preceded it, called LANDOC, which contained more than 300,000 documents in a variety of different text and image formats. EDMS also contains and documents added to Documentum is a Brief Bank repository where FTC staff can find briefs and documents filed by the FTC in federal court cases.

Documentum is "the system" referenced in this Privacy Impact Assessment (PIA). While many of the documents in the system are public, the system itself is non-public, with access limited to FTC staff and approved contractors.

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

The FTC Act, the Commission's Rules of Practice, and other laws and regulations that the Commission enforces permit the collection of the information. For more information, see http://www.ftc.gov/ogc/stats.

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)*:_____ _____
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

The system stores numerous Commission documents that contain various items of PII, including names, addresses, telephone and fax numbers, e-mail addresses, financial information such as bank account information, credit information and Social Security numbers.

2.1(a) FTC Brief Bank

The FTC Brief Bank is located in Documentum's work product repository. The Brief Bank contains public versions of FTC briefs and other filings in federal court cases.

Access to the Brief Bank is limited to staff in OGC, BC, BCP, the Bureau of Economics, the Office of International Affairs and the Office of Public Policy. Staff in these organizations have read-only access to all documents in the Brief Bank. Users will not be able to edit the documents in the Brief Bank (they are final versions) but can copy and paste to documents they create outside of Documentum. A limited number of users in OGC and BCP have additional rights to add content (documents and metadata) to and delete it from their organization's folder. A limited number of users in BC (and possibly a limited number of users in the Regional Offices) will also have these rights for the BC folder.

[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.

2.2 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.

Documents in EDMS include law enforcement related documents and other types of documents. Examples of law enforcement related documents in the system include compulsory process documents (e.g., subpoenas and civil investigatory demands); investigative hearing transcripts, transcripts of depositions in adjudicative proceedings, transcripts of adjudicative hearings and trials; briefs and other documents filed in adjudicative proceedings; orders entered in adjudicative proceedings; briefs and other documents filed in federal court cases; federal court orders to pay consumer redress and financial statements from individuals ordered to pay redress; Federal Register Notices of proposed consents; petitions related to cease and desist orders and FTC responses; and attachments to filings made through the HSR (Hart-Scott-Rodino) Electronic Filing System.

Examples of other documents in the system include staff memoranda to the Commission and other staff memoranda; Congressional correspondence; Federal Register notices of rulemakings; requests for formal and informal advisory opinions and FTC responses; news releases; and speeches given by FTC officials.

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

Information in the system is collected, used, disseminated and maintained in order for the Commission to perform its law enforcement functions and other activities. For example, FTC staff collects and uses the information to investigate anticompetitive practices and to enforce statutes protecting consumers from fraudulent, deceptive, and unfair practices in the marketplace. In addition, the information is used in a variety of other ways, such as to assist with consumer redress and respond to Congressional correspondence. As described in the System Overview, agency documents that are stored in the system allow the staff to access, track, and search. In addition, this system can assist in responses to FOIA and other disclosure requests by providing search and access capability for responsive documents.

All uses of the data are relevant and necessary to the purpose for which it was collected. The system does not collect any new information that is not already collected by the agency for its law enforcement programs and other activities.

All users of the system have a level of access determined by their need-to-know, with the lowest level of access needed to perform their work.

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

Information in the system is obtained by FTC staff in connection with the agency's law enforcement and other activities.

Source of Data	*Type of Data Provided & How It Is Collected*
FTC staff, via voluntary processes	In some instances, this information is provided voluntarily, such as when individuals submit comments in rulemaking proceedings or send correspondence to Congress which is then forwarded to the FTC, and when investigatory targets agree to provide information to the Commission in lieu of compulsory process. In some instances, individuals – for example, third parties in investigations and witnesses in administrative and federal court matters – provide about other individuals.
FTC staff, via compulsory process and other law enforcement processes	FTC staff also obtain information in response to compulsory process, such as subpoenas and civil investigatory demands, or via discovery in administrative databases, other law enforcement agencies, and commercial databases such as Lexis/Nexis.
Commercial or public sources	Some of the data in the system used for law enforcement and other Commission activities is commercial or publicly available. For example, commercial databases as well as publicly available sources (e.g. telephone and address directories) may be used to provide information on investigatory targets. The FTC is not engaged in data mining and the data is not used for this purpose.

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*
Agency staff and contractors	Agency staff and contractors who require information in support of FTC law enforcement and other activities, and in order to respond to FOIA and other disclosure requests, will have access to the information, subject to the access restrictions. A Manager's written authorization is required before an agency employee receives access to Documentum.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
Others outside the agency.	While nobody outside the FTC has access to Documentum, documents stored in Documentum (such as letters to the commission) may be forwarded outside the commission as needed (for instance, if the letter was wrongly directed to the FTC)

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.

Contractors have access to Documentum and BriefBank. For contractors, a contracting officer's technical representative (COTR) or Administrative Officer at the request of the COTR, must provide written authorization before the contractor can gain access to the network. In addition, the officer must specifically authorize access to Documentum and the issuance of an Oracle password (needed to access Documentum). The Documentum administrator will grant access if the proper documentation is submitted and concurs with the decision. Access is only granted to contracts if there is a business need.

To manage content, a limited number of contractors in RIM and OS can add or delete metadata and documents in the system. An OCIO contractor who supports the system administrator has full access rights to all documents and metadata in the system. All FTC contractors sign Non-Disclosure Agreements.

In addition, agency staff and contractors are subject to security background checks, and access to the system is controlled by user ID and passphrase combination, a separate log in for Documentum with user ID and an Oracle password, and electronic or network controls (e.g. firewalls). Staff and contractors receive annual training on, and are required to adhere to, written FTC policies protecting sensitive PII and non-public information including that contained in the system.

☐ Not Applicable.

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.

The contractors referenced in 3.2 above are covered by the FTC's Breach Notification Response Plan.

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.

Wherever possible, the FTC provides notice to individuals about its policies regarding the use and disclosure of information at the time the information is collected. For information that is collected pursuant to a request from the FTC, notice is provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). For those occasions where the FTC cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the FTC provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its PIAs.

☒ 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*):_____

☐ Notice is not provided (explain): _____

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)?

The opportunity or right depends on how the information is collected. For example, those who provide information pursuant to compulsory process do not generally have a right to decline to provide the information. However, individuals who file public comments or requests for advisory opinions, or who end inquiries to members of Congress (which become part of the Congressional correspondence in the system) provide information about themselves voluntarily and could choose to decline to provide such information.

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

An individual may make a request under the Privacy Act for access to information maintained about themselves in this system or other systems at the FTC. Individuals must follow the FTC's Privacy Act rules and procedures which are published in the Code of Federal Regulations at 16 C.F.R 4.13. Access to the information under the Privacy Act is subject to certain exemptions. In addition, there are many public documents in the system that also appear on the FTC's website.

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.

See 4.3 above.

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?

The system is a document management system that maintains agency documents already collected or generated in the course of agency business. Accordingly, these documents are placed into the system "as is" without verifying their accuracy or timeliness. The accuracy and timeliness of the information in such documents is verified, however, as necessary and appropriate at the time they are collected, generated, or used by the agency (e.g., in law enforcement investigations or litigation).

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.

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure the information contained in the system is appropriately secured.

The following auditing, testing, and technical safeguards are in place to prevent misuse of data:

- Access Enforcement – There is active monitoring and testing of access privileges. For instance, reports can be run to verify access and privileges. In addition, audit functions can be turned on to monitor document viewing.
- Least Privilege – Only the appropriate folder and file rights are assigned to a user to perform his/her function.
- Unsuccessful Login Attempts – The system automatically locks a user's account when the maximum number of unsuccessful attempts is exceeded.

All FTC staff and contractors with access to the system can do so at a read-only permission level. As noted previously, access to documents and their metadata is further restricted based on a need to know. The system administrator (an employee in OCIO) and an OCIO contractor who supports the system administrator, have full access rights to all documents and metadata in the system in order to assist with maintenance of and enhancements to the system and, in some instances, content management. In order to manage system content, a limited number of staff and contractors in RIM and the Office of the Secretary (OS) can add or delete documents and metadata in the system, with the exception of redress orders and the accompanying financial statements, attachments to

premerger filings, speeches of agency officials, and OCIO task sections of the system. OS staff and contractors have no access to the Brief Bank. A limited number of RIM staff and contractors have the right to add content (documents and metadata) to and delete it from the Brief Bank during its initial deployment. A limited number of users in OGC and BCP have rights to add content (documents and metadata) to and delete it from their organization's folder in the Brief Bank. A limited number of users in BC (and possibly a limited number of users in Regional Offices) will also have these rights for the BC folder. In addition, OCIO contractors who are project managers, as well as OCIO staff can initiate project management workflows in Documentum and attach technical documents to these workflows. The initiators and a limited number of OCIO staff can create multiple versions of these documents and modify the documents' metadata as needed to manage the project.

Currently the permissions granted allow "read only" access for the majority of users, though a comparatively small number of users have rights to add and delete documents and metadata. The system administrator, a contractor in OCIO, who supports the system administrator have full access rights to all documents and metadata in the system in order to assist with maintenance of and enhancements to the system and, in some instances, content management.

Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical controls associated with need-to-know and least privilege, ensuring that users have no more privileges to data than required to complete their official duties.

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

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

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?

Most documents in the system are copies of paper records that scanned in the system, validated, and then destroyed 90 days after validation of the electronic records. The electronic records in the system are covered by the FTC NARA-approved records disposition schedule N1-122-09-1. However, along with the corresponding indexing system, Matter Management System 2 (MMS2), the data is retained by the agency until no longer needed for agency business.

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.

The system is not made available for access or disclosure through any public website.

☒ Not Applicable

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***
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes, or could disclose Documentum information without authorization.	Most documents in the system are also coded by type in order to limit access to particular classes of system users (e.g., Commissioners and their office staff; or Commission staff in a specific organization). Access to documents in the Brief bank is controlled by the user groups assigned to the Brief Bank's folders. The system administrator and an OCIO contractor who supports the system administrator maintain the user groups. Staff and contractors receive annual training on, and are required to adhere to, written FTC policies protecting sensitive PII and non-public information including that contained in the system.
Unauthorized access to Documentum	The FTC also does not make user access to the application available to anyone other than authorized FTC employees and contractors. The system is not accessible to outside parties (e.g., other law enforcement agencies).

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

Access to the system is controlled by user ID and passphrase combination, a separate log in for Documentum with user ID and an Oracle password, and electronic or network controls (e.g. firewalls).

Most documents in the system are also coded by type in order to limit access to particular classes of system users (e.g., Commissioners and their office staff, or Commission staff in a specific organization).

Any user with access to a document in the Brief Bank can click on "history" under the "properties" tab and see who added the document to the Brief bank and when. Any user can also see if one of the limited number of users with add rights has checked a document and checked it back in – for example to substitute a PDF version of the document for an MSWord version. The system administrator (an employee in OCIO) and an OCIO contractor who supports the system administrator can also run reports of who deleted a document from the Brief Bank and when. As noted, all documents in the Brief Bank are public filings and most users have read-only access. The technology employed in Documentum, including the audit feature, does not raise any special privacy concerns.

For more information about technical privacy safeguards, see section 5.2.

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).

Documentum is covered by an existing Privacy Act System of Records Notice (SORN). See FTC-VII-6, Document Management and Retrieval System – FTC. http://www.ftc.gov/foia/listofpaysystems.shtm

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 FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure the information contained in the system is appropriately secured. The Privacy Office routinely collaborates with system/application owners as part of its Privacy Continuous Monitoring Strategy to ensure that the information in PIAs, including this one, is accurate and to mitigate any privacy risks, as needed. Members of the public with questions or comments on the FTC's privacy practices may contact the Chief Privacy Officer using the contact information at ftc.gov/privacy.