Federal Trade Commission
Privacy Impact Assessment

Microsoft Office 365 (O365) Multi-Tenant & Support Service

July 2019

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

Microsoft Office 365 (O365) is a Software-as-a-Service (SaaS) product that combines the familiar Office Productivity suite with online versions of Microsoft's next-generation communications and collaboration services. O365 will allow the FTC to simplify administration of licenses and subscriptions to services at an enterprise level and facilitate system-wide user management, password administration, and oversight of security controls. The initial O365 implementation centers on Outlook, with other applications to follow. This privacy impact assessment (PIA) evaluates privacy implications for FTC's use of the cloud-based O365 service products listed below:

- OneDrive
- Outlook
- SharePoint
- Word
- Excel
- PowerPoint
- OneNote
- Access

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)*: Email messages and office documents stored in O365 may contain PII voluntarily submitted by end users. PIN/Password may also be stored.
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

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.

The FTC houses a variety of non-PII information in O365 depending on the needs and purposes of the offices that use this software. Documents that could be created or housed in O365 applications may include a variety of law enforcement documents, internal staff memoranda, Congressional correspondence, and Federal Register notices of Rulemakings.

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

Information in O365 applications is collected, used, disseminated, and maintained for the Commission to perform its law enforcement, policy, personnel management, and other activities. Due to the range of supported services, personal information may be present

[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.

for a variety of reasons in the course of conducting communication, collaboration, creation and management of records, and information security.

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*
FTC Staff and Contractors	FTC staff and contractors upload data that has been created or obtained in connection with the Commission's law enforcement, policy and other activities. User-created content may also include information in the user's profile, emails, calendar, and other information voluntarily stored within O365.
Members of the Public	The public's information is not collected directly by O365. However, information provided by and pertaining to members of the public may be stored in O365. These individuals may include consumers, witnesses or individual targets in law enforcement matters, individuals commenting on agency rulemakings and workshops, etc.

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*
FTC Staff	Access to O365 is restricted to authorized FTC end users. All end users must adhere to the FTC Rules of Behavior. Access to the information stored within O365 is dependent on the particular business purpose and the access permissions granted to a specific user. For example, system administrators may have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions.
Contractors	FTC may have contractor support within program areas, and these contractors will have access to the information in O365 as required to perform their duties.
Office of Inspector General (OIG)	Under appropriate circumstances, data showed within O365 or O365 log data may be provided to the OIG for auditing or law enforcement purposes.

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.

Authorized FTC contractors have access to information in O365, when necessary. Some authorized FTC contractors have access to O365 simply as users, and one or more authorized FTC contractors has access to certain administrative functions.

All FTC contractors are required to sign NDAs, complete security and privacy training prior to obtaining access to any FTC systems, and complete annual security and privacy training to maintain network access and access to those systems.

☐ 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.

Contractors who access O365 are subject to the same rules and policies as FTC staff. Contractors must also follow the reporting and other procedures in the FTC's Breach Notification Response Plan.

☐ Not Applicable.

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 timely and effective notice to the public and/or to individuals about activities that impact privacy. For information that is collected pursuant to a request from the FTC, notice is provided as part of that request. The FTC's Privacy Act statements are included on all forms, websites, and other instruments by which Privacy Act information is collected from individuals, either in written or oral form. 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, including this one.

☒ 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. The FTC does not use O365 to collect information, including PII, directly from the public. However, FTC staff and contractors use O365 in furtherance of the FTC's law enforcement or policy mission. Information collected through other sources, which includes PII, is maintained in O365. Please see the list of the FTC's Privacy Impact Assessments for more information on how the FTC collects information from the public

For example, FTC staff may include information obtained from a consumer complaint filed with the FTC's Consumer Sentinel Network in a document (Word) or an email (Outlook) that includes PII from members of the public. In that instance, the consumer has notice and opportunity to decline to provide information prior to filing the complaint. However, when PII obtained from a company pursuant to compulsory process is included in O365, individuals may not have received notice or been provided with an opportunity to decline to provide the 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 and retrieved according to personal identifier by the FTC about themselves in the FTC's Privacy Act systems, including any data stored in O365 applications. The FTC's Privacy Policy provides links to the FTC's System of Records Notices (SORNs), as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals seeking access 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.

As specified above in Section 4.3, to the extent the Privacy Act applies, the FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the FTC, including any information that may be stored in O365. 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 about themselves in Privacy Act systems, including data in O365. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file FOIA requests for agency records about them (if they are not exempt from disclosure to them under those laws). Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly. Where

appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

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?

Due to the nature of the system and the anticipated broad use of these services across the enterprise, information that is stored in O365 generally will not be checked for accuracy, completeness, accuracy, completeness, or currency. It is the responsibility of the user to ensure the completeness, accuracy and currency of data at the time it is created or used.

Information that is used by the FTC as part of its law enforcement and other activities will be reviewed for accuracy and timeliness as required by the particular activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures).

System administrators ensure user information is complete and accurate for access control through Active Directory (AD) authentication, but will not ensure that data created or entered by end users is complete, accurate, or current. AD is updated immediately when a user account is disabled or terminated. User contact information is removed once the user account is deleted. Within the organization, users have the ability to enter their own information and to ensure that it is current.

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.

FTC's O365 implementation is not accessible to anyone outside the FTC. The principle of least privilege is used to grant access to FTC staff and contractors, and user actions are tracked in the O365 audit logs. All potential FTC staff and contractors are subject to background investigations and suitability reviews in accordance with OPM guidance. Before accessing O365, these individuals must first attend new employee orientation and successfully complete the FTC's Information Security Awareness and Privacy training. All staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's annual privacy and security training.

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?

The FTC does not use PII to conduct O365 system testing, training, or research.

☐ 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?

Information in the FTC O365 cloud instance is retained and destroyed in accordance with applicable FTC policies and procedures, as well as with the FTC records disposition schedule and General Records Schedules approved by the National Archives and Records Administration (NARA). FTC staff receive training and reminders about their records and destruction obligations. All information will be securely and irreversibly disposed of/destroyed in accordance with applicable FTC policies and procedures, OMB, NARA, and NIST regulations and guidelines.

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.

No. The FTC's O365 configuration is an intranet site accessible through the FTC network, and only FTC staff and contractors have access to it. Session and persistent cookies keep O365 from timing out while a user is logged into it, but these cookies are used for internal purposes only. O365 does not collect information directly from the public.

☐ 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***
Misuse of data by authorized users	Prior to receiving access to the FTC's network, all users must agree to the FTC Rules of Behavior, which includes consent to monitoring and restrictions on data usage.
Unauthorized system access	All users must have an FTC account and government-issued personal identity verification (PIV) card to access O365. FTC's user identity management processes include authentication with Active Directory (AD) to control and manage access restrictions to authorized personnel on an official need-to-know basis. The FTC utilizes a combination of technical and operational controls to reduce risk in the O365 environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention

	policies. As a FedRAMP-approved cloud service provider, O365 undergoes regular reviews of its security controls.
Data leakage	The contract between FTC and O365 does not allow the service provider to access, review, audit, transmit, or store FTC data, which minimizes privacy risks from the vendor source.

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

User access is managed through the FTC's Active Directory (AD) infrastructure, which uniquely identifies, authenticates, and applies permissions to authorized user sessions based on FTC policies and procedures. This allows the FTC to leverage organizational multifactor authentication solutions, including FIPS-201 compliant PIV cards, already deployed to meet internal identification and authentication requirements. The use of AD also allows automatic enforcement of certain policies and requirements, such as password complexity and maximum-log in attempts, for organizational users.

Additionally, FTC security policies require automated monitoring of information system components with regard to flaw remediation.

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).

O365 does not itself require a SORN; however, SORNs that cover documents and records in O365 that are considered part of Privacy Act systems are accessible at https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems.

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 administrative and technical controls described in section 5.2 of this document provide assurance that the collection, use, and maintenance of the information will be conducted as described in this PIA. This PIA aligns with the FTC's existing privacy policies and procedures.