NASA Policy Directive

NPD 1382.17K
Effective Date: March 28, 2022
Expiration Date: March 28, 2027

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: NASA Privacy Policy

Responsible Office: Office of the Chief Information Officer

1. POLICY

a. NASA's policy is to:

(1) Protect all forms of controlled unclassified information (CUI), including personal information.

(2) Comply with Federal law and regulations governing management of all personal information collected, used, maintained, and disseminated by or on behalf of NASA in electronic or non-electronic form.

(3) Use the National Institute of Standards and Technology (NIST) Privacy Framework as a foundation to manage enterprise privacy risk.

(4) Ensure all collections of CUI (including personal information as defined in Attachment A of this NASA Policy Directive (NPD)) are assessed for applicability of, and management and protection in compliance with, Federal laws, regulations, and Government-wide policies listed in this directive.

(5) Ensure all collections of personal information gathered by or on behalf of NASA leverage Agency-specific individual identifiers, such as the Universal Uniform Personal Identification Code (UUPIC).

(6) Avoid, to the greatest extent possible, the use of Social Security Numbers (SSNs), and, in instances where SSNs are already in use, review collections of SSNs for possible SSN removal or replacement.

2. APPLICABILITY

a. This NPD is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to all contractors providing services to NASA, including the Jet Propulsion Laboratory (a Federally Funded Research and Development Center), grant recipients, or parties to agreements to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. This NPD is applicable to all NASA users (e.g., civil servants and contractors) who collect personal information in support of Agency projects, programs, and missions.

c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

3. AUTHORITY

a. Privacy Act of 1974, 5 U.S.C. § 552a.

b. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501 et seq.

c. Paperwork Reduction Act of 1995(PRA), 44 U.S.C. § 3501 et seq.

d. Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq.

e. E-Government (e-Gov) Act of 2002, 44 U.S.C. § 3601 et seq.

f. Creating Advanced Streamlined Electronic Services (CASES) for Constituents Act, which became Public Law 116-50, 133 Stat. 1073 (2019).

g. Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

4. APPLICABLE DOCUMENTS AND FORMS

a. SSN Fraud Prevention Act of 2017 Pub. L. 115-59, 131 Stat. 1152 (2017).

b. NPR 1382.1, NASA Privacy Procedural Requirements.

5. RESPONSIBILITY

a. The NASA Administrator:

(1) Designates NASA Senior Agency Official for Privacy (SAOP).

(2) Delegates to the SAOP the overall responsibility and accountability for ensuring NASA's implementation and management of personal information protections, including the Agency's full compliance with Federal laws, regulations, and Government-wide policies relating to information privacy listed in this directive.

b. The SAOP:

(1) Has the primary responsibility for maintenance and implementation of the Agency's privacy policy.

(2) Carries out the NASA Administrator's delegated responsibilities for privacy.

(3) Ensures that Privacy Threshold Analysis (PTAs) and Privacy Impact Assessments (PIAs) are conducted as required by NPR 1382.1, NASA Privacy Procedural Requirements.

(4) Provides OMB with PIAs for planned Information Technology (IT) systems and for collections of information from the public as required.

(5) Appoints the NASA Chief Privacy Officer (CPO).

(6) Delegates oversight, governance, training, and implementation responsibilities for privacy activities to the CPO.

(7) Appoints the NASA Privacy Act Officer (PAO).

(8) Establishes and chairs the Data Integrity Board if and when NASA conducts or participates in a data-matching program as described in and in accordance with 5 U.S.C. § 552a.

(9) Ensures that NASA adheres to the SSN Fraud Prevention Act of 2017.

c. The NASA CPO:

(1) Responds to privacy-related actions issued by Congress or external Agencies.

(2) Oversees, manages, and implements Federal privacy laws, regulations, and NASA and Government-wide policies identified in this directive as directed by the SAOP.

(3) Ensures compliance with privacy provisions contained in Federal statutes, including the collection, maintenance, use, and dissemination of personal information.

(4) Develops and maintains NASA privacy policies, procedural requirements, handbooks, and memoranda.

(5) Develops and coordinates submission of Agency privacy reports to OMB.

(6) Provides final quality reviews of all Agency PIAs, System of Records Notice (SORNs), communications, and other documents routed to the SAOP for signature.

(7) Develops and manages privacy training and outreach to meet Federal requirements.

(8) Maintains an Agency state of heightened awareness regarding the protection of NASA personal information.

d. The NASA Privacy Act Officer:

(1) Provides management and oversight to ensure NASA compliance with 5 U.S.C. § 552a requirements.

(2) Ensures inclusion of Privacy Act requirements in NASA policy and training.

(3) Conducts regular review and reporting activities as required by 5 U.S.C. § 552a and OMB directives.

(4) Communicates and coordinates with CPO, Center Privacy Managers and other NASA personnel with respect to privacy requirements.

(5) Provides guidance and writing assistance in the development or revision of SORNs.

e. Center Directors and the Director of Headquarters Operations:

(1) Ensure Center compliance with this directive and requirements in NPR 1382.1.

(2) Designate a Center Privacy Manager (CPM).

f. Center Chief Information Officers (CIOs):

(1) Ensure Center adherence to NASA privacy policy requirements through the respective CPM.

(2) Ensure the CPM is aware of all privacy related information compromises and incidents, whether potential or confirmed.

g. CPMs:

(1) Serve as the Center's expert on all Center-related NASA privacy matters, including overseeing, managing, and implementing NASA privacy policies and procedural requirements.

(2) Serve as the interface between the NASA CPO, PAO, and Center personnel on privacy matters.

(3) Coordinate and provide the Center's privacy reports as required by the NASA CPO.

(4) Ensure that Information Owners (IOs), Information System Owners (ISOs), and Data Owners (DOs) perform required information collection assessments and aid in the development of any required documentation.

(5) Lead at the Center level all Agency-wide privacy reviews and actions.

(6) Participate in and provide oversight, guidance, and support for Privacy Breach Response Team (BRT) activities, investigations, and reporting of personally identifiable information (PII) breach incidents.

(7) Notify and regularly update the NASA CPO throughout the BRT process.

(8) Conduct a local exercise or support the Agency annual Privacy BRT exercise in accordance with NPR 1382.1, and report completion and lessons learned to the NASA CPO.

h. Heads of Mission Directorates and Mission Support Offices (MSOs) may appoint a Mission Privacy Point of Contact (MPPOC).

(1) The MPPOC will have the same privacy accountability as that of the CPMs as outlined in this and other Agency privacy directives, and have direct accountability to act as a liaison in providing support to the CPM for Center-wide privacy related reporting and operational activities.

(2) If a Mission Directorate or MSO PPOC is not appointed, the CPM fulfills the privacy responsibilities for the Mission Directorate and fulfills MSO activities located at, or under the cognizance of, the related Center.

i. IOs, ISOs, and DOs:

(1) Ensure all personal information collected under their purview is properly identified and assessed via the PTA or PIA.

(2) Ensure personal information is identified and assessed during the earliest possible milestones of, and at each key decision point throughout the life-cycle management process.

(3) Validate that the personal information is protected, managed, and controlled prior to any active collection of, or creation of, new collections.

(4) Ensure personal information collected by their system(s) is securely transmitted and stored in accordance with Federal laws, regulations, and Government-wide and NASA policy and procedural requirements listed in this directive.

(5) Conduct and support annual privacy review and reduce activities for collections of PII and SSNs.

(6) Respond to Agency-level reporting requirements and data call actions in support of annual FISMA and other

Federal or Agency requirements.

j. All NASA Users (civil servant and contractor):

(1) Protect all personal information (both electronic and non-electronic) for which the user is responsible or that is in the user's custody.

(2) Ensure any electronic storage or dissemination of personal information is encrypted when in electronic transmission or at rest, as detailed in NPR 2810.1, NASA Information Security Policy.

(3) Ensure that any personal information in the user's custody is disseminated only to those individuals who have the need to know.

(4) Immediately report directly to the NASA Security Operations Center (SOC) any PII potential or confirmed breaches (e.g., loss, inappropriate access, or unauthorized disclosure) upon discovery.

(5) Complete required privacy training upon reporting to NASA for employment either as a civil servant or contractor, and annually thereafter.

6. DELEGATION OF AUTHORITY

The NASA SAOP is delegated authority to carry out the functions and exercise the authority vested in the Administrator to implement, oversee, and manage privacy policy within the Agency pursuant to the authorities cited above.

7. MEASUREMENT/VERIFICATION

None.

8. CANCELLATION

NPD 1382.17J, NASA Privacy Policy, dated June 29, 2016.

/s/ Bill Nelson
Administrator

ATTACHMENT A: DEFINITIONS

Data-matching program, any computerized comparison of two or more automated systems of records.

Information in identifiable form (IIF), in accordance with section 208(d) of the e-Gov act, IIF is defined as "... any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

In accordance with OMB Memorandum M-03-22, IIF "... is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements (i.e., indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors."

Information Owner (or Data Owner) has statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

NASA User is any explicitly authorized patron of a NASA information system. The NASA user includes, but is not limited to, civil servants and contractors.

Personally identifiable information, in accordance with M-07-16, PII "... refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual,

such as date and place of birth, mother's maiden name, etc."

In accordance with M-10-23, "... [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual."

Sensitive PII. Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For purposes of NASA policy, sensitive PII excludes personal information collected and or maintained by NASA employees and contractors for personal rather than NASA business purposes, as allowed under NID 2540.138, Acceptable Use of Government Furnished Information Technology Equipment, Services, and Resources.

Examples of such excluded data include contact information for family, relatives, and doctors.

NASA defines PII commensurate with OMB Memoranda M-17-12 with further definition as it applies to sensitive and non-sensitive PII. Sensitive PII is well defined above however, Non-Sensitive PII, though it is PII, is information that is available through commonly available public sources, the disclosure of which cannot reasonably be expected to result in personal harm or embarrassment.

Significant Change. For the purposes of this policy as it applies to PTAs and PIAs, significant change is defined as any change that constitutes new uses of existing information being collected, application of new technologies (such as non-electronic collection to electronic, implementation of persistent tracking technology (cookies), how information is collected or managed, from whom the information is to be collected, duration of information retention, how the information is being collected (e.g., forms, electronic or non-electronic), or any change to the application, system, Web site, Web application or information collection (including change in NASA responsible official, information owner or system owner), that effects how the information is stored, managed, and protected.

Privacy Act Information is any information which is subject to the requirements established by the Privacy Act of 1974 and NASA Privacy Act Regulations, 14 CFR pt. 1212 - The Privacy Act sets forth extensive requirements for the management of personal information contained in a system of records (SOR), where such information is routinely retrieved by a name or personal identifier unique to the individual.

Privacy Information (or personal information, is any information, which falls within the definitions of IIF, PII, or Privacy Act as described herein.

Laws, regulations, and guidance documents provide various terms and definitions used to describe privacy or personal information. These include: personally identifiable information or PII, personal information, Privacy Act records, and IIF.

ATTACHMENT B. ACRONYMS

CIO Chief Information Officer

CISO [Center] Chief Information Security Officer

COPPA Children's Online Privacy Protection Act

CPM Center Privacy Manager

CPO Chief Privacy Officer (synonymous with Privacy Program Manager (PPM))

CUI Controlled Unclassified Information

DO Data Owner

e.g. exempli gratia (for example)

FISMA Federal Information Security Modernization Act

IIF Information in Identifiable Form

IO Information Owner

ISO Information System Owner

JPL Jet Propulsion Laboratory

NASA National Aeronautics and Space Administration

MPPOC Mission Directorate and Mission Support Offices (MSOs) Appointed Privacy Point of Contact

MSO Mission Support Office

NIST National Institute of Standards and Technology

NITR NASA Information Technology Requirement

NPD NASA Policy Directive

NPR NASA Procedural Requirement

OCIO Office of the Chief Information Officer

OMB Office of Management and Budget

PAO [NASA] Privacy Act Officer

PIA Privacy Impact Assessment

PII Personally Identifiable Information

PRA Paperwork Reduction Act

PPM Privacy Program Manager (synonymous with Chief Privacy Officer (CPO))

PTA Privacy Threshold Analysis (sometimes previously referred to as Information Privacy Threshold Analysis or Initial Information Privacy Threshold Analysis)

SAISO Senior Agency Information Security Officer

SAOP Senior Agency Official for Privacy

SOC Security Operations Center

SORN System of Records Notice

SSN Social Security Number

U.S.C. United States Code

UUPIC Universal Uniform Personal Identification Code

ATTACHMENT C. REFERENCES

C.1. OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites.

C.2. OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.

C.3. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

C.4. OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy.

C.5. OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications.

C.6. OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

C.7. NID 2540.138, Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources.

C.8. National Institute of Standards and Technology (NIST) Special Publications

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.