Introduction to The Privacy Act

Defense Privacy and Civil Liberties Office

dpclo.defense.gov

Introduction

The Privacy Act (5 U.S.C. 552a, as amended) can generally be characterized as an omnibus "Code of Fair Information Practices" that regulates the collection, maintenance, use, and dissemination of personally identifiable information (PII) by Federal Executive Branch Agencies.

Broadly stated, the purpose of the Privacy Act is to (1) balance the government's need to maintain information about individuals with the right of individuals to be protected against unwarranted invasion of their privacy and (2) to limit the unnecessary collection of information about individuals.

The Act focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies.
2. To grant individuals increased rights of access to agency records maintained on themselves.
3. To grant individuals the right to seek amendments of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
4. To establish a code of "Fair Information Practices" which requires agencies to comply with statutory norms for collection, maintenance, use, and dissemination of records.

Applicability

The Privacy Act applies to:

- Federal Agencies;
- Living U.S. Citizens or legal aliens lawfully admitted for permanent residence.

Code of Fair Information Practices

- **Collection limitation.** There must be no personal data record keeping systems whose very existence is secret.
- **Disclosure.** There must be a way for an individual to find out what information about an individual is in a record and how it is used.
- **Secondary usage.** There must be a way for an individual to prevent information about an individual that was obtained for one purpose from being used or made available for other purposes without his consent.
- **Record correction.** There must be a way for an individual to correct or amend a record of identifiable information about the individual.
- **Security.** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

What is Covered by the Privacy Act?

The Privacy Act governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A **system of records** (SOR) is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual, such as an SSN.

Disclosing Personally Identifiable Information

General Disclosure Prohibition: No agency shall disclose any record that is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

Restrictions on Disclosing Privacy Act Records

The individual subject of the file must provide consent to allow disclosure of information from a Privacy Act system to a third party; however, there are 12 exceptions to this consent rule.

Exceptions to the "No Disclosure to Third Parties Without Consent Rule"

1. To employees with a legitimate need-to-know;
2. When the FOIA requires release;
3. For a "routine use" identified in the System of Records Notice (SORN) that has been published in the Federal Register;
4. To the Census Bureau for purpose of conducting the census;
5. For statistical research and reporting in which individuals will not be identified;
6. To the National Archives and Records Administration;
7. To civil or criminal law enforcement under U.S. control;
8. For compelling circumstances affecting the health or safety of the individual;
9. To either House of Congress;
10. To the Comptroller General;
11. Pursuant to a court order (a subpoena signed by a judge); or
12. To a consumer reporting agency in accordance with the Debt Collection Act.

Information Sharing Concerns

Need-to-Know

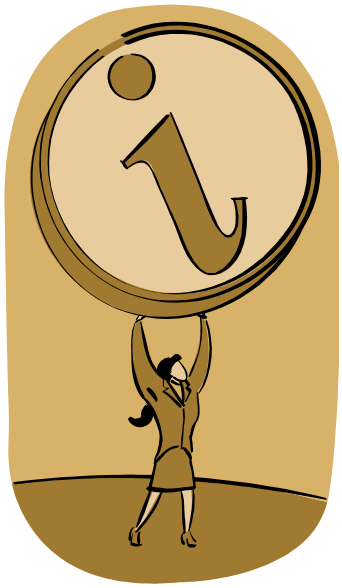
Need-to-know is the authorized, official need based on assigned duties and responsibilities to have access to information that is protected under the Privacy Act.

There are three cases when a need-to-know may be established:

- Official business
- Statutory
- Information sharing

If a need-to-know has not been or cannot be established, the following actions should be taken:

- Do not share the information in question.
- If information has already been inappropriately released, notify your manager immediately, as this is a breach.



Privacy Act Notices and Advisories

As related to the Privacy Act, a record is any item, collection, or grouping of information about an individual that is maintained by an agency. This includes, but is not limited to, education, financial transactions, medical history, and criminal or employment history and that contains an individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

System of Records

A System of Records is a group of records in which the data about the individual is retrieved by a personal identifier (E.g., SSN, date of birth, biometric data, etc.).

System of Records Notice

A System of Records Notice is a formal notice published in the *Federal Register*. The notice:

- Advises the public of the data collection;
- Clearly states what data may be collected and how it will be used, stored, shared, and safeguarded.

System of Records Notice

The following fields are required in a System of Records Notice:

- System Identifier
- System Name
- System Location
- Categories of Individuals Covered by the System
- Categories of Records in the System
- Authority for Maintenance of the System
- Purpose(s)
- Routine Uses of Records Maintained in the System, Including Categories of Users and the Purpose of Such Uses
- System Policies and Practices relating to:
    - Storage
    - Access
    - Retrievability
    - Retention and Disposal
    - Safeguards

Privacy Act Statements and Advisories

Privacy Act Statements and Advisories are required when an individual is asked to:

- Provide their SSN or other personal data.
- Confirm that their data is current and correct

Privacy Act Statement and Advisories allow the individual to make an informed decision about providing their data.

Privacy Act Statements are required when PII will be filed within a System of Records.

Privacy Act Advisories are required when

- You will retrieve the data by a non-personal identifier (geographic data, date, etc.) AND
- You are collecting SSNs.

Additional Guidance on Privacy Act Notices, Statements and Advisories

- All collections are voluntary.
- Collections may be listed as "mandatory" only of:
    - The person is required by law to provide the data AND
    - The person is subject to a penalty for refusing.

Sample Privacy Act Statement

Privacy Act Statement

Authority: 5 U.S.C. 301, Department Regulations; 5 U.S.C. 6122, Flexible Schedules; E.O. 10450, Security Requirements for Government Employees; and E.O. 9397* (SSN), as amended.

Purpose: Information is collected to verify your eligibility to access controlled facilities and for issuing badges for use in entering facilities.

Routine Use: Information may be disclosed for any of the DoD "Blanket Routine Uses" published at http://privacy.defense.gov/blanket_uses.shtml. Contact your local Privacy Officer for further details.

Disclosures: Voluntary; however, failure to provide the information may result in our inability to grant your access to our facilities.

***** Privacy Act Statements **must** contain a valid authority for the collection of Social Security Numbers (if applicable to the system). Although Executive Order 9397 must be listed as the last authority for systems that collect SSNs, there must be another authority for the collection of SSNs, such as a Federal law or a DoD Directive or Regulation.

Sample Privacy Act Advisory

Privacy Act Advisory

Authority: 18 U.S.C. 1029, Access device fraud; E.O. 9397* (SSN), as amended.

Disclosure of your SSN is voluntary: However, if you fail to provide your SSN, we will be unable to grant you access to the XYZ database.

Uses to be made of your SSN: Your SSN will be compared against the master list of employees for the sole purpose of positively identifying you. It will not be shared with anyone outside DoD. Once we have confirmed your identity, we will destroy this form.

This data collection will not become part of any Privacy Act System of Records.

* Privacy Act Statements **must** contain a valid authority for the collection of Social Security Numbers (if applicable to the system). Although Executive Order 9397 must be listed as the last authority for systems that collect SSNs, there must be another authority for the collection of SSNs, such as a Federal law or a DoD Directive or Regulation.

Placement of the Privacy Act Statement or Advisory

For Forms: Preferably at the top of the page immediately under the title of the form.

For Surveys: Opening page of the survey instrument OR in a cover memo appended to the survey instrument.

For Web Pages: Conspicuously on the screen that collects the data.

For Other Modalities: Boldly referenced at the top of the collection device.

Civil and Criminal Penalties

Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect on the subject of the record may result in:

Civil penalties: (Applies to the Agency)

- The cost of actual damages suffered ($1,000.00 minimum)
- Costs and reasonable attorney's fees

Criminal penalties: (Applies to the Individual Employee)

- A misdemeanor charge
- Maximum fine of $5,000.00

Safeguarding Personally Identifiable Information

A combination of administrative, physical, and technical safeguards are needed to protect the personally identifiable information entrusted to the Department. Below are some safeguards to keep in mind:

Administrative Safeguards

- Ensure that every recipient of PII has a need-to-know. Before sending an e-mail, verify that the distribution list is only for those individuals with a need-to-know.
- Validate the use of information against the purpose of the collection documented in the System of Records Notice.
- SORN Managers should keep SORNs up to date by reviewing them at least every two years.
- Ensure telephone conversations are private. Be aware of your surroundings. Land lines are preferred over cell phones.
- Consult your Component Privacy Officer before collecting PII.
- Properly mark all copies of documents containing PII as "Privacy Act Sensitive."
- Collect, use, maintain, and disseminate data that is accurate, complete, relevant and timely.

Technical Safeguards

- Encrypt all e-mails that contain PII.
- Use only DoD-approved software on your computer.
- Do not use flash ("thumb") drives for transporting PII.
- Never use personal equipment to store PII.
- Ensure that information is from a government authorized source.

Safeguarding Personally Identifiable Information (Continued)

Physical Safeguards

- Use locks to secure PII when stored.
- Dispose of records according to established schedules in the SORN or procedures established by the National Archives and Records Administration.
- System Managers should maintain a record of the movement of hardware and electronic media in their control, including to whom the equipment was issued, the date of issuance, and the date of return.
- Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

References

- Defense Privacy and Civil Liberties Office—http://dpclo.defense.gov
- DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
- DoD Regulation 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- DA&M Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009

Definitions

Access

The ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any system resource.

Authorization

A narrowly tailored permission to use and disclose only the specific PII identified for the limited purpose requested. Authorizations must have a limited duration and may only be relied upon for that period of time.

Biometrics

Physiological and/or behavioral characteristics that are measurable and can be used to verify the identity of an individual.

Biometric Authentication

The method of matching a person's claimed identify to their biometric and one or more other security technologies.

Biometric Identifiers

Examples of some common Biometric Identifiers are fingerprints, voice patterns, face geometry, hand geometry, retinal scans, signatures, and typing patterns.

Breach

Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected.

Confidentiality

Information that is not made available or disclosed to unauthorized individuals, entities, or processes.

Computer Matching Agreement

An agreement which governs the comparison of two or more automated system of records using a computer. Manual comparisons of printouts of two automated data bases are not included in this definition. A matching program covers the actual computerized comparison and any investigative follow-up and ultimate action by covered agencies.

Data

A sequence of words or symbols to which meaning may be assigned.

Data Integrity

Condition existing when data is unchanged from its source and has

not been accidentally or maliciously modified, altered, or destroyed.

Data Authentication

The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.

Decryption

The process of transforming cipher text into readable text.

Disclosure

The release, transfer, access to, or divulging of personal information by any mean of communication in any manner (electronic, oral, or written) outside the entity holding the information to any person or private entity.

Encryption

The process of changing plaintext into ciphertext for the purpose of security or privacy.

Individual

Any living citizen of the United States or any alien lawfully admitted for permanent residence.

Personally Identifiable Information (PII)

Information about an individual that identifies, links, relates, or is unique to, or describes the individual, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc.

Examples of PII include:

- Social Security number, mother's maiden name, birth date
- Personal phone number, e-mail address, home address
- Biometric, personal, medical, and financial information

Record

Any item, collection, or grouping of information about an individual that is maintained by an agency. This includes, but is not limited to, education, financial transactions, medical history, and criminal or employment history and that contains an individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Routine Use

A disclosure of a record that must be compatible with the purpose for which the information in the record was collected and must be identified to the public.

System of Records (SOR)

A group of records under the control of any agency from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned

to the individual.

System of Records Notice (SORN)

A formal document stating the information in the System of Records is collected and identifies what data the agency intends to collect, how the data will be used and safeguarded, who will have access, and other details. The Agency has a responsibility under the Privacy Act to publish in the Federal Register a notice of the existence and description of a collection about individuals.

Defense Privacy and Civil Liberties Office
1901 South Bell St., Suite 920
Arlington, VA 22202-4512

(703) 607-2943
dpo.correspondence@osd.mil