Trigger Points Indicating Privacy Act Considerations

If you answer 'yes' to any of these questions, consult your DoD Component Privacy Official for potential Privacy Act requirements.

1. Are you collecting PII?

2. Are you retrieving information from that collection of PII by a personal identifier, e.g., name, social security number?

3. Are you unable to identify a published system of records notice that correlates with the purpose for your collection?

(http://dpclo.defense.gov/privacy)

4. Are you creating a collection of PII by merging information from two or more existing information systems?

5. Are you conducting a computerized comparison of Federal automated systems with Federal records?

Defense Privacy & Civil Liberties Office
1901 South Bell Street, Suite 920
Arlington, VA 22202

(703) 607-2943

Defense Privacy & Civil Liberties Office

The Privacy Act of 1974:

What Senior Leaders Need to Know

Think Privacy!

What is the purpose of the Privacy Act?

The Privacy Act of 1974 provides protection (safeguards) for individuals against an invasion of privacy by federal agencies.

What are the agency's responsibilities when collecting information on individuals?

Collect only the minimum amount of information necessary to accomplish an authorized purpose.

Maintain only information about an individual that is
– Complete – Accurate – Timely – Relevant

Whenever collecting personal information directly from an individual, provide the individual with a Privacy Act Statement informing him or her
– Whether the provision of the information is voluntary or mandatory
– The purpose for which the information is intended
– Any routine uses of the information
– The effects, if any, of not providing all or any part of the requested information.

Ensure accurate and up-to-date systems of records notices (SORNs) are published in the Federal Register.

Allow individuals access to and the means to correct records about themselves when those records are maintained in a nonexempt Privacy Act system of records.

Exercise written agreements when conducting computerized comparisons of (1) two or more automated systems of records or a system of records with non-Federal records, or (2) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

What information is covered by the Privacy Act?

Personally identifiable information (PII) under the control of a DoD Component and held within a system of records falls under the protection of the Privacy Act

What is PII?

Personally identifiable information (PII) is defined as information which can be used to distinguish or trace an individual's identity to a specific individual such as name, social security number, date and place of birth, mother's maiden name, biometric records and other personal information linked to an individual.

What is a system of records?

Any group of records where information is retrieved by the name of the individual or a personal identifier is referred to as a system of records.

What is a system of records notice (SORN)?

A SORN is published in the Federal Register informing the public that an agency is maintaining a system of records. The SORN describes the source of the information; the kind of information being collected and on whom; the authority allowing the collection; where, how, and how long the information will be maintained; and routine uses of the information.

Think Privacy!

What are routine uses?

A routine use is a disclosure of PII from a system of records to a recipient outside of DoD. Routine use disclosures must be consistent with the purpose(s) for which the information was collected and must be published in the Federal Register.

Under what conditions (exceptions) of the Act may I disclose information inside and outside DoD without consent from the individual to whom the record pertains?

NOTE: Number 1. below applies to internal DoD uses; all others reflect disclosures outside DoD.

1. The disclosure is to an agency employee who normally maintains the record and needs to know the information in the performance of duty;
2. The disclosure is made under the Freedom of Information Act;
3. The disclosure is for a routine use;
4. The disclosure is to the Census Bureau for the purposes of a census survey;
5. The disclosure is to someone who has adequately notified the agency in advance that the record is to be used for statistical research or reporting, and the record is transferred without individually identifying data;
6. The disclosure is to the National Archives and Records Administration as a record of historical value;
7. The disclosure is to an agency of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, and if the record is provided in response to a written request by the head of the agency;
8. The disclosure is made where there are compelling circumstances affecting someone's health or safety, and the person whose health or safety is affected is sent a notification of the disclosure;
9. The disclosure is made to Congress, or any committee or subcommittee within Congress;
10. The disclosure is made to the Comptroller General in the course of the duties of the General Accounting Office;
11. The disclosure is made pursuant to a court order;
12. The disclosure is made to a consumer reporting agency

How do I execute agreements for computerized matches?

The Defense Privacy and Civil Liberties Office (DPCLO) coordinates computer matching agreements. Contact DPCLO for guidance on procedures and assistance.

Think Privacy!

What are the agency's responsibilities when information is breached?

A breach results when there is an actual or possible loss of control, unauthorized disclosure, or unauthorized access to information contained in a system of record.

Examples of breaches include persons (including DoD personnel) without an authorized need to know accessing PII, computer hacking, the loss of paper records and the theft of laptops containing PII.

Upon Suspicion of or Awareness of an Actual Breach		
Report To:	U.S. Computer Emergency Readiness Team (US-CERT)	Within 1 hour of discovering that a breach of PII has occurred.
	Senior DoD Component Privacy Official	Within 24 hours
	Defense Privacy and Civil Liberties Office	Within 48 hours
Notify:	Affected Individuals	As soon as possible but no later than 10 working days after a breach is discovered and the identities of the individuals are ascertained.