ENCLOSURE A19

Army Regulation 25–22

Office Management

The Army Privacy and Civil Liberties Program

Headquarters
Department of the Army
Washington, DC
30 September 2022

UNCLASSIFIED

1–9. Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs), originally developed in 1973 by the Department of Health, Education, and Welfare, formed the conceptual core for the PA of 1974. Army activities should apply these principles when handling records containing PII.

a. Access and amendment. Provide individuals with appropriate access to PII and appropriate opportunity to correct or amend their records that contain PII.

b. Accountability. Hold personnel accountable for complying with measures that implement the FIPPs and applicable privacy requirements, and appropriately monitor, audit, and document compliance. Clearly define the roles and responsibilities with respect to PII for all employees and contractors, and provide appropriate training to all employees and contractors who have access to PII.

c. Authority. Create, collect, use, process, store, maintain, disseminate, or disclose PII only with the proper authority to do so and identify this authority in the appropriate SORN.

d. Minimization. Create, collect, use, process, store, maintain, disseminate, or disclose PII only when it is directly relevant and necessary to accomplish a legally authorized purpose, and only maintain PII for as long as is necessary to accomplish the purpose.

e. Quality and integrity. Create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

f. Individual participation. Involve the individual in the process of using PII and, to the extent practicable, seek individual consent for creating, collecting, using, processing, storing, maintaining, disseminating, or disclosing PII. Establish procedures to receive and address individuals' privacy-related complaints and inquiries.

g. Purpose specification and use limitation. Provide notice of specific purpose for which PII is collected and only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

h. Security. Establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

i. Transparency. Be transparent about information policies and practices with respect to PII, and provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

1–10. General provisions

a. Consider privacy and civil liberties in the development, implementation, and review of new or existing regulations, policies, and initiatives.

b. Protect the privacy and civil liberties of Soldiers, Army civilian employees, and the public (persons and organizations not affiliated with DoD) to the greatest extent possible, consistent with DoDD 5200.27 and operational requirements.

c. Ensure that neither the Army nor any subordinate command or agency will collect, report, process, maintain, or disseminate any information on how an individual, group of individuals, or association exercises fundamental rights, specifically including the freedoms of speech, assembly, press, and religion, except when—

(1) Specifically authorized by statute; or

(2) Expressly authorized by the individual, a group of individuals, or an association on whom the record is maintained; or

(3) Pertinent to and within the scope of an authorized law enforcement, intelligence collection, or counterintelligence activity.

d. Have adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege that the Army has violated their privacy or civil liberties.

e. Individual privacy rights policy. Although deceased individuals do not have PA rights, family members or next-of-kin may have limited privacy rights with respect to the release of information regarding the death and the funeral arrangements of the deceased individual. Family members often use the deceased individual's Social Security number (SSN) or DoD identification (ID) data number for Federal entitlements. Also, the Health Insurance Portability and Accountability Act (HIPAA) extends protection to certain medical information contained in a deceased individual's medical records. Appropriate safeguards must be implemented to protect the deceased individual's PII and PHI.

f. Reprisals or the threat of reprisals are prohibited against individuals who make complaints or disclose information that indicates a possible violation of privacy protections or civil liberties in the administration of the Army's programs and operations to privacy or civil liberties officials. Appropriate disciplinary action under law and regulation will be considered for all violations.

1–11. Special handling provisions

a. Send privacy protected data electronically via email and the world wide web according to the following guidelines:

(1) The PA requires that appropriate technical safeguards be established based on the media used to ensure the security of the records and to prevent compromise or misuse during transfer.

(2) Sensitive PII, such as SSNs, is to be transmitted via encrypted email or password protected. When sending PA protected information within the Army across encrypted or dedicated lines, ensure that—

(a) Each addressee has an official "need to know." Remove any recipient without a "need to know" from all addressee fields.

(b) Information protected by the PA is marked "Controlled Unclassified Information (CUI)" to inform the recipient of limitations on further dissemination. For example, add CUI to the beginning of an email message, along with appropriate language such as the following: "This message contains personal or privileged information which is protected under the PA of 1974, as amended. Do not further disseminate this information without the permission of the sender."

(c) For email with an attachment, include a statement similar to the following: "If you are not the intended recipient, please delete this email including any attachments, and notify the sender that you have done so."

(d) Unclassified information associated with the PA and identified as needing safeguarding is considered CUI. It requires access control; handling, marking, dissemination control; and other protective measures for safeguarding. CUI information may qualify for withholding from public release based on a specific FOIA exemption.

(e) For additional information about CUI marking and dissemination instructions, refer to DoDI 5200.48.

(3) Add appropriate privacy and security notices at major website entry points. Refer to AR 25–1 for requirements on posting privacy and security notices on public websites.

(4) Ensure Army websites are in compliance with policies regarding restrictions on persistent and third-party cookies. The Army prohibits both persistent and third-party cookies.

(5) Add a Privacy Act Advisory (PAA) on websites with host information systems soliciting PII, even when not maintained in a PA SOR. The PAA informs the individual as to why the information is being solicited and how it will be used. Post the PAA on the website where the information is being solicited, or to a well-marked hyperlink. Example wording is as follows: "Privacy Act Advisory—Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used."

b. Protect paper records containing personal identifiers such as name and SSN as follows:

(1) Only those records covered by a SORN may be arranged to permit retrieval by a personal identifier (for example, an individual's name or SSN). AR 25–400–2 requires all records thus covered to include the SOR identification number on the record label to serve as a reminder that the information contained within must be safeguarded.

(2) Use Standard Form (SF) 901 (CUI Cover Sheet) for individual records not contained in properly labeled file folders or cabinets (for example, log books or training materials).

1–12. Civil liberties

a. Civil liberties are fundamental rights and freedoms enjoyed by all individuals that cannot be restricted or deprived, without due process. Due process requires that these liberties can only be curtailed for a proper governmental objective and the affected individual must be given notice of the proposed restriction or deprivation, and an opportunity to argue before a neutral decision maker that the civil liberties should be preserved.

b. The U.S. Constitution protects civil liberties. While the U.S. Constitution explicitly identifies certain civil liberties, others can also be expressed, explicitly or implicitly, by state or federal law or judicial interpretation.

c. Civil liberties include, but are not limited to the following:

(1) Freedom of speech (First Amendment).

(2) Freedom of religion (First Amendment).

(3) Freedom to assemble (including peaceful protest) (First Amendment).

(4) Freedom of the press (First Amendment).

(5) The right to keep and bear arms (Second Amendment).

(6) Freedom from unreasonable searches and seizures (Fourth Amendment).

(7) The prohibition against deprivation of life, liberty, or property without due process of law (Fifth Amendment).

(8) The right not to answer incriminating questions (Fifth Amendment).

(9) Freedom from the deprivation of rights not included in the U.S. Constitution but retained by the people (Ninth Amendment).

(3) Justification.

b. After appropriate staffing and approval by the Secretary of the Army, or authorized designee, the rule is forwarded to DPCLFD for publication in the FR (see DoDI 5400.11). No exemption may be invoked until these steps have been completed. Army SORNs citing exemptions are codified in 32 CFR 310. For the most current listing of Army SORNs, see the ARMD website at https://www.rmda.army.mil/privacy/sorns/armypublishedsorn.html.

Chapter 5
Handling and Safeguarding Personally Identifiable Information

5–1. Collecting personally identifiable information

a. When collecting PII, Army administrators and other users of PII must observe the provisions and guidelines described in this section. This section applies to Army military, civilians, and contractors.

b. General provisions for collecting PII are as follows:

(1) The Army collects PII directly from the subject of the record whenever possible. This is especially important when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.

(2) When an Army activity asks an individual for his or her PII that will be maintained in a SOR, the activity must provide the individual with a Privacy Act Statement (PAS). A PAS notifies individuals of the authority, purpose, and use of the collection, whether the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information. See paragraph 5–3 of this regulation when soliciting SSNs for any purpose.

c. A PAS must be prepared and administered based on the following guidelines:

(1) The Federal statute or EO that authorizes collection of the requested information.

(2) The principal purpose or purposes for which the information is to be used.

(3) The routine uses that will be made of the information.

(4) Whether providing the information is voluntary or mandatory.

(5) The PAS includes language that is explicit, easily understood, and concise.

(6) A sign is displayed in areas where people routinely furnish this kind of information, and a copy of the PAS is made available upon request by the individual.

(7) The individual reads but does not sign the PAS.

(8) A PAS must include the following items:

(a) Authority. Cite the specific statute or EO, including a brief title or subject that authorizes the DA to collect the PII requested.

(b) Principal purpose(s). Cite the principal purposes for which the information will be used.

(c) Routine use(s). Cite the routine uses for which the information may be used. The routine use should be specific and must align with the routine use included in the applicable SORN. If none, the language to be used is: "Routine Use: None." However, the "Blanket Routine Uses" set forth at the beginning of the Army's compilation of systems of records notices may apply.

(d) Disclosure: Voluntary or Mandatory. Include in the PAS specifically whether furnishing the requested PII is voluntary or mandatory. A requirement to furnish PII is mandatory only when a Federal statute, EO, or other law specifically imposes a duty on the individual to provide the information sought, and when the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of or prerequisite to granting a benefit or privilege and the individual has the option of requesting that benefit, then the collection is voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought must be listed as a consequence of not furnishing the requested information.

d. Some acceptable means of administering the PAS are as follows, in the order of preference:

(1) Below the title of the media used to collect the PII (positioning the PAS so the individual will observe the PAS before providing the requested information).

(2) Within the body with a notation of its location below the title.

(3) On the reverse side with a notation of its location below the title.

(4) Attached as a tear-off sheet.

(5) Issued as a separate supplement.

e. The usage and elements of a PAS are described in appendix B.

f. Include a PAS on a website if the site requires information directly from an individual and the information is retrieved by his or her name or personal identifier.

g. When collecting PII from third parties, it may not be practical to collect personal information directly from the individual in all cases. Some examples of when third-party collection may be necessary include—

(1) To verify information.
(2) To solicit opinions or evaluations.
(3) To use another source when the subject cannot be contacted.
(4) At the request of the subject individual.

h. When asking third parties to provide information about other individuals, advise them of—

(1) The purpose of the request.
(2) Their rights to confidentiality as defined by the PA.

Note. Consult with your servicing Staff Judge Advocate for potential limitations to the confidentiality that may be offered.

i. Promises of confidentiality must be prominently annotated in the record to protect from disclosing any information provided in confidence based on 5 USC 552a(k)(2), 5 USC 552a(k)(5), or 5 USC 552a (k)(7).

5–2. Safeguarding personally identifiable information

a. The PA requires establishment of proper administrative, technical, and physical safeguards to—

(1) Ensure the security and confidentiality of records (for example, to periodically verify that only personnel with a current and valid need to know have access to shared drives and document management systems).

(2) Protect against any threats or hazards to the subject's security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness.

b. Ordinarily, PII must be afforded at least the protection required for information designated "Controlled Unclassified Information." PA data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of record content during processing, storage, transmission, and disposal.

c. With the growing use of websites, the proliferation of social media, and the increasing risks of and cases of identity theft, the dimensions for the safeguarding of data have expanded exponentially in recent decades. Webmasters and web maintainers must apply appropriate privacy and security policies to respect user privacy. As specified in AR 25–1, organizations must screen their websites and display a privacy and security notice in a prominent location on at least the first page of all major sections of each website. Each website must clearly and concisely inform visitors to the site about any information the activity collects, why it is collected, and how it will be used.

d. Each privacy and security notice must clearly and concisely inform visitors to the site what information the activity collects about individuals, why it is collected, and how it will be used. If PII is requested in the notification and record access procedures, but not collected or listed in the categories of records, the reason for requesting the PII must be explained.

e. If the SSN is used for verification purposes, the custodian of the record must state "SSN required for verification purposes only."

f. The DA recognizes the importance of safeguarding PII in all forms of electronic media in addition to paper media. For information on approved Army use of social media, see website: https://www.army.mil/mobile/socialmedia.html.

5–3. Protecting Social Security numbers

a. When soliciting or using SSNs, Army administrators and other users of SSNs observe the provisions and guidelines described in this section and DoDI 1000.30. It is unlawful for any Federal, State, or local Government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to give their SSN unless the law requires disclosure, or a law or regulation adopted prior to January 1, 1975, required the SSN or if DA uses the SSN to verify a person's identity in a SOR established and in use before that date. EO 9397 (issued prior to January 1, 1975 and amended by EO 13478) authorizes the Army to solicit and use the SSN as a numerical identifier for individuals in most federal systems. However, the SSN should only be collected as needed to perform official duties. EO 9397 does not mandate the solicitation of SSNs from Army personnel as a means of identification.

b. Upon entrance into military service or civilian employment with DA, individuals are asked to provide their SSN. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial medical, and other official records. After an individual has provided his or her SSN for the purpose of establishing a records, the PAS is not required if the individual is only requested to furnish or verify the SSN for identification purposes in connection with the normal use of his or her records. If the SSN is to be used for a purpose other than identification, the individual must be informed whether disclosure of the SSN is mandatory or voluntary; by what statutory authority the SSN is solicited; and what uses will be made of the SSN. This notification is required even if the SSN is not to be maintained in a PA SOR.