DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON BAVARIA
UNIT 28130
APO AE 09114-8130

AMIM-BAH (1oo)

MEMORANDUM FOR All USAG Bavaria Military and Civilian Personnel

SUBJECT: USAG Bavaria Policy Memorandum #13, Privacy Act Procedures

1. References.

a. AR 25-22, The Army Privacy Program and Civil Liberties Program

b. DoD 5400.11-R, Department of Defense Privacy Program

2. It is everyone's responsibility to ensure that our privacy practices and procedures are followed. The Privacy Act promotes, and safeguards Personally Identifiable Information (PII) maintained by a system of records. The collection, storage, use, maintenance, processing, dissemination, and disclosure of personal information must comply with the Privacy Act of 1974 (5 U.S.C. § 552a).

3. This policy applies to all military, civilian, host nation, and contractor personnel assigned to and/or under the operational control of the Garrison Commander.

4. Garrison personnel must collect only the minimum amount of PII that is legally authorized and necessary to support their operations. The records must be maintained in an authorized system of records and disposed of in accordance with the Army Records Information Management System (ARIMS). Personal information must be timely, accurate, complete, and relevant to the collection purpose. Additional requirements for collecting PII may include Privacy Impact Assessment (PIA), privacy policy or notice, privacy act statement, and System of Record Notice (SORN).

5. We must ensure the security and confidentiality of information and records, protect against possible threats or hazards and permit access only to authorized persons. All records (paper and electronic) will be protected as prescribed in DOD Regulation 5400.11-R (DOD Privacy Program) and AR 25-22 (The Army Privacy Program).

6. In accordance with AR 25-22, supervisors must ensure new personnel receive initial duty-specific privacy act training. All Army personnel must complete annual refresher training. The online Privacy and Civil Liberties Initial/Annual Course and Specialized Training Course can be accessed through the Army Training Information System (https://learn.atis.army.mil/).

7. PII breaches (lost, stolen or compromised PII) must be reported to the chain of command and the Garrison privacy official immediately. The enclosed printout from the RMDA website describes all additional reporting requirements.

8. Teleworker and remote workers will implement appropriate physical, administrative, and technical safeguards IAW with this Policy Memorandum to protect the security and confidentiality of PII.

9. Disciplinary Action. Individuals who repeatedly mishandle PII or violate their responsibilities to ensure the protection of PII will be subjected to administrative, punitive, or disciplinary action, or could also result in civil and criminal action.

10. Individuals who perceive an alleged violation or want to file a complaint should contact the Garrison Privacy Official.

11. POC is the Garrison Privacy Official, Christine Nunez, 526-4465, or email christine.a.nunez4.ln@army.mil.

Encl.

STEPHEN C. FLANAGAN
COL, SF
Commanding

PII Home
Examples of PII
Safeguarding PII
Protective Measures
PII Breaches
Report a PII Incident
PII Breach Reporting Process Flowchart
Privacy Act Tracking System (PATS)
Risk Determination
Notifications
Post-Incident Activity
Resources
Definitions
FAQs
Guidance
Point of Contact

Reporting a Personally Identifiable Information (PII) Incident

All Army Commands (ACOM), Army Service Component Commands (ASCC), Direct Reporting Units (DRU), Army Staff, Program Executive Offices (PEO), and Army activities are required to ensure all suspected or actual loss, theft, or compromise of PII regardless of physical or electronic form is reported in accordance with the following procedures.

1. Report the incident immediately to your first line supervisor, your Privacy Official, and if cyber-related to your Information Technology division as well.

   Note:

   a. If the actual or suspected incident involves PII occurs as a result of a contractor's actions, the contractor must also notify the Contracting Officer Representative immediately.

   b. If the incident involves a Government-authorized credit card, the issuing bank should be notified immediately.

2. Report all cyber-related incidents involving the actual or suspected breach/compromise of PII **within one hour** of discovery to the United States Computer Emergency Readiness Team (US-CERT) by completing and submitting the US-CERT report at https://www.us-cert.gov/forms/report.

   The notification to US-CERT regarding an electronic breach should include as much information as possible, however, **reporting should not be delayed to gain additional information.** See US-CERT Federal Incident Notification Guidelines for reporting requirements. The US-CERT report format provides the user with various drop-down answer options and the ability to skip sections to identify areas that do not apply to non-technical breaches.

   Note: Make sure you record the US-CERT number assigned to the breach. You will need this to complete section 1d of the Breach of Personally Identifiable Information (PII) Report via PATS.

3. Report both electronic and physical related incidents to the Army Privacy Office (APO) within 24 hours of discovery by completing the Breach of Personally Identifiable Information (PII) Report via PATS.

   When completing the Breach of Personally Identifiable Information (PII) Report in PATS **do not include any PII**, such as names of individuals. Reportable information includes:

   Date of breach, date discovered, and date reported to United States Computer Emergency Readiness Team (US-CERT)

   US-CERT number and Component Internal Tracking Number (if applicable)

   Component and Office Name

   Point of contact information including name, duty phone, and office mailing address

   Narrative description of breach (up to 150 words) including:

   - The parties involved in the breach **(do not use names of individuals)**
   - The media used such as email, info-sharing, paper records, or equipment
   - Type of breach: loss, theft, or compromise
   - Immediate steps taken to contain the breach

   Mitigating actions taken (up to 150 words) including:

   - Whether the breach was intentional or inadvertent
   - Any lessons learned

   Number of individuals affected (including numbers of Soldiers, civilians, and contractors involved)

   The type of PII compromised such as SSN, PHI, and financial information

   Any additional information as indicated on the form

   If computer access is not available, PII incidents can be reported to a 24/7 Army toll free number at 1-866-606-9580 or US-CERT at (888) 282-0870 which is also monitored 24/7.

4. For additional reporting requirements, consult with your Privacy Official and follow your activity's guidance for reporting PII incidents.

5. Submit updates to APO through PATS. Also submit updates to US-CERT, your Privacy Official and appropriate individual(s) within your Activity as information becomes available. **Note:** US-CERT requires that any updates to the initial report are to be provided via email to soc@us-cert.gov and the assigned US-CERT number must be referenced in the subject line.

APO will report the incident to DPCLTD within 24 hours upon being notified that a loss, theft, or compromise has occurred. When an incident includes an actual or suspected compromise of Personal Health Information (PHI), APO will also report the incident to the Defense Health Agency (DHA) Privacy Office within 24 hours of discovery.

WHAT HAPPENS AFTER A SUSPECTED OR ACTUAL BREACH HAS BEEN REPORTED?

See Risk Determination

Encl - PII Breach Reporting Procedures from RMDA Website