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

AMIM-BAG-ZA

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, 30 Sep 2022

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 are required to collect the minimum amount of Personally Identifiable Information (PII) as legally authorized and necessary for their operations. All digital PII records must be securely stored in the designated Army Material Command (AMC) Microsoft A365 SharePoint Online (SPO) document library. The collected information must be kept timely, accurate, complete, and relevant. Further requirements may include a Privacy Impact Assessment (PIA), a privacy policy or notice, a Privacy Act statement, and a 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. Situational teleworkers 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

DEREK G. DROUIN
COL, AR
Commanding

CHECK SHEET

United States Army Garrison (USAG) Bavaria
Personally Identifiable Information (PII) – Privacy Act Potential Breach Reporting Form

Report Date:	
Time of Report:	

Employee Information

Name (Last, First):	
Job Title/Rank:	
Directorate/Office:	
Office Symbol:	
Phone Number:	
Email:	
Kaserne/Installation:	
Building Number:	
Office Number:	

Potential PII / Privacy Act Data Breach Information

**For questions about filling out the form, please email:usarmy.wiesbaden.id-europe.mbx.G1--Privacy-Office@army.mil*

Please identify the type of suspected data breach:	Paper/Hard Copy: ☐ IT/Local Computer: ☐ SharePoint Online: ☐ Website: ☐ Other (please describe):
Please describe, in detail, the website, SharePoint Online link, IT folder name, file cabinet location and/or specifics of the suspected data breach location:	

United States Army Garrison (USAG) Bavaria
Personally Identifiable Information (PII) – Privacy Act Potential Breach Reporting Form Continued

Please describe the scope of employees affected (how many per each hiring category):	GS: NAF: LN: Contractors: Volunteers: *If applicable: Retirees: Family Members: Any additional Comments:
Please describe the type(s) of data suspected in the potential breach (list all types):	
Location of where you were, when you first suspected the potential breach:	Kaserne/Installation: Building Number: Office Number: *If off-post, please describe: Confirm Date: Confirm Time:
Has anybody already contacted S6/IMO for data containment? Has anybody already contacted the CMD Team?	Yes: ☐ No: ☐ Yes: ☐ No: ☐
What additional assistance do you need at this time, aside from waiting for advisement from the Privacy Officer once the incident is reported/assessed?	
Please report any immediate actions that have taken place:	

Please digitally sign here:

*Email completed form to: *usarmy.wiesbaden.id-europe.mbx.G1--Privacy-Office@army.mil*

United States Army Garrison (USAG) Bavaria
Personally Identifiable Information (PII) – Privacy Act Potential Breach Reporting Form Continued

Report Received Information

Date Report Received:	
Time Report Received:	
Person Receiving the Report:	
Additional Notes:	

USAG Bavaria Privacy Officer Signature: