



PRIVACY IMPACT ASSESSMENT (PIA)

For the

VAT RP EUROPE - EUROPE VALUE ADDED TAX RELIEF PROGRAM

United States Army Europe (USAREUR) IMCOM - G9

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

- DoD Instruction 5100.64, DoD Foreign Tax Relief Program
- DoD Directive 5530.3, International Agreements
- DoD Directive 5525.1, Status of Forces Policy and Information
- USEUCOM Directive 45-8 stipulates that the Designated Military Commander for Tax Relief in Germany is the Commander USAREUR.
- the Supplementary Agreement with Federal Republic of Germany to the NATO Status of Forces Agreement and Host Nation directives require monitoring of the program to prevent abuse (tax evasion).
- Army in Europe Regulation AER 215-6

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of this electronic collection is to maintain information required to issue Value Added Tax-Relief Forms (VAT Forms) to verified/authorized US Forces members so they can effect tax-free purchases on the Host Nation Economy and to facilitate tracking of purchases to monitor for abuse (tax evasion). Types of personal information are: Full name, DoDID, APO address, local address, email, place of work, family member names, which forms were issued (serial numbered), what purchases were made (amount, what product/service). The PII collected is also necessary to effect wage garnishments procedures for debt owed to the MWR fund when individuals do not pay bills (when a member uses a VAT form to make a purchase but does not pay the bill the issuing VAT office is liable).

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

PII is collected by users providing data on paper forms. VAT office employees input the information through a user application that is stored in a SQL database. The user application has undergone peer code review, DISA STIG assessments for Application Development, and a formalized Certificate of Networkiness process for vetting new applications onto the DoDIN. The user application has been submitted for a CoN. The SQL database storing the PII has a DITPR 16616 and AITR DA207134.

The Enterprise SQL as a Service (ESaaS) backend is an accredited information system which has been created specifically for the purpose of hosting Department of Army application databases in a consolidated environment. There are hundreds of Information Assurance guidelines implemented to protect the data contained within, IAW strict DISA Security Technical Implementation Guides. Key Protective Measures: AES Encryption standards are used to protect data at rest, as well as data in transit. Clearly defined access controls for both logical and physical access have been implemented. ESaaS is housed in an approved Army Datacenter, and it is administered by trained professionals for the technology. ESaaS is also highly redundant system, making it fault tolerant from the power grid, to the servers it is comprised of, to the data centers it resides in.

Additional information about ESaaS can be obtained by reading the System Security Plan.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Other (e.g., commercial providers, colleges).

Specify.

Host Nation law enforcement and fiscal agencies will not have direct access to the system. If requested by the Host Nation, the proponent will provide only statistical data or scrubbed excerpts of data that the US Forces are required to share in accordance with the NATO-SOFA SA (must be specific to a particular law enforcement case) after legal review by USAREUR Office of the Judge Advocate.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals fill out the VAT Application Form AE Form 215-6A, which contains a privacy act clause/statement and advises the individual that he/she is not required to provide the data.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes

No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

By filling out and signing the VAT Application Form AE Form 215-6A, the individual consents. If the individual chooses not to fill out and sign the VAT Application Form AE Form 215-6A, no consent is given and no data is collected by this system.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

Authority: Title 10 USC Section 3012 and the Supplementary Agreement to the NATO SOFA, Article 67, paragraph 3a(a)(i); AE Regulation 215-6/USAFE Instruction 34-102, on individual tax-relief procedures in Germany.
Purpose(s): For MWR/Service Fund custodians to use in obtaining tax-relief and to verify eligibility of applicants for tax-relief.
Routine use(s): To provide information needed to process documents for tax-relief purchases and to verify the requester is authorized tax relief support.

Mandatory or voluntary disclosure and effect on individuals not providing information: Disclosure of information is mandatory. Tax relief cannot be obtained without the requested information.

Statement of Understanding and Hold-Harmless Clause The undersigned acknowledges responsibility for the cost of any goods or services purchased with tax-relief documents obtained from the U.S. Forces CMWRF/Services Fund and agrees to hold harmless the U.S. Government and the CMWRF/Services Fund from any suit, liability, claim, action, or loss as a result of the purchase of such goods or services. The undersigned further understands and agrees to advise the CMWRF/Services Fund immediately if any part of the transaction cannot be completed and also agrees to return the white copy of AE Form 215-6B to a tax-relief office when the tax-exempt transaction has been completed. The undersigned further understands and agrees to safeguard all tax-relief documents, preclude unauthorized use by non-ID-card personnel, return unused documents to a tax-relief office before departing the command, and not exceed the €2,499.99 limit on unpriced purchases.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.