DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY NAPLES ITALY
PSC 817 BOX 1
FPO AE 09622-0001

17 July 2023

NAVSUPPACT NAPLES POLICY ON PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY ACT DATA

An individual's privacy is a fundamental legal right that must be respected and protected. As you know, the loss of Personally Identifiable Information (PII) can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy, maintains PII, we have a special duty to protect that information from loss and misuse. In fact, Title 5, Section 552a of the United States Code, (the Privacy Act) mandates that all federal employees, including Department of Defense (DoD) contractors collecting PII for a DoD system of records, safeguard PII.

Careless loss or compromise of PII not only leads to identity theft and other criminal behavior, but prevents our people from focusing on daily tasks and overall mission. We rely on our people to accomplish the mission; they rely on those that have access to their PII to safeguard it. This is a leadership responsibility. Communication, awareness and training are fundamental in resolving inadvertent compromise of PII.

PII should be treated as "For Official Use Only" (FOUO). Unauthorized disclosure of this information may result in civil and criminal penalties. If you are not the intended recipient of PII or believe you have received information in error, do not copy, disseminate or otherwise use the information.

The NAVSUPPACT Naples Official PII/Privacy Act policy is as follows:

DEFINITION OF PII. PII is any information, characteristic, or combination thereof that can be used to distinguish or trace an individual's identity. Examples include but are not limited to: name, Social Security number (SSN), date of birth, home address, home phone number, personal e-mail address, financial information, fingerprints, photograph, medical information, leave balances, mother's maiden name, and civilian National Security Personnel System (NSPS) data.

COLLECTING PII. PII collected, used, maintained, or disseminated by NAVSUPPACT Naples will be: (1) relevant and necessary to accomplish a lawful DoD purpose required by statute or Executive order; (2) collected to the greatest extent practicable directly from the individual. He or she will be informed as to why the information is being collected, the authority for collection, how it will be used, whether disclosure is mandatory or voluntary, and the consequences of not providing that information; (3) relevant, timely, complete, and accurate for its intended use.

NAVSUPPACT Naples will maintain no records on how an individual exercises rights guaranteed by the First Amendment to the Constitution of the United States, except: (1) when specifically authorized by statute; (2) when expressly authorized by the individual that the record is about; (3) when the record is pertinent to and within the scope of an authorized law enforcement activity, including an authorized intelligence or administrative investigation.

NAVSUPPACT NAPLES POLICY ON PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY ACT DATA (cont'd)

PROTECTIVE MEASURES. PII collected and maintained by NAVSUPPACT Naples will be protected using appropriate administrative, technical, and physical safeguards based on the media (e.g., paper, electronic) involved. Protection will ensure the security of the records and prevent compromise or misuse during maintenance, including working at authorized alternative worksites.

Information Technology Equipment

Never leave your laptop unattended.

Keep your laptop secured at all times.

All mobile electronic equipment must have full disk encryption.

Mark all portable media devices with "FOUO, Privacy Sensitive."

As a best practice, do not create, store or transmit PII on IT equipment when the information is not encrypted.

Ensure PII resides only on government furnished IT equipment.

Never store PII on personal devices.

Do not maintain PII on a public web site.

E-Mail

E-mail containing PII must be digitally signed and encrypted using DoD-approved certificates.

As a best practice, ensure the e-mail subject line contains "FOUO Privacy Sensitive" if the document contains PII.

Ensure the body of the e-mail contains the following warning, "FOUO. Privacy Sensitive Information. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

Ensure you have the correct e-mail addresses before sending.

Ensure you are sending correct attachment when forwarding via email.

Printed Materials, Scanners, and Fax Machines

Verify printer location prior to printing documents containing PII.

Promptly retrieve documents as soon as they are printed.

Ensure the destination of scanned documents before scanning.

Ensure the fax number prior to faxing documents with PII.

Ensure someone is standing by on the receiving end of the fax.

Ensure all printed documents with PII are properly marked with "FOUO, Privacy Sensitive."

As a best practice, transport/hand carry PII documents in a double wrapped container/envelope. Use a DD Form 2923 "Privacy Act Data Cover Sheet" as a cover.

Disposal

Dispose of documents containing PII by making them unrecognizable by shredding or burning.

As a best practice, prior to turn in, ensure all hard drives are properly marked, physically destroyed, and actions documented.

Do not discard documents containing PII in trash or recycle bins.

Copiers and printers use hard drives and must be properly sanitized.

NAVSUPPACT NAPLES POLICY ON PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY ACT DATA (cont'd)

Network Shared Drives

Make sure that controls are in place to limit access to files/folders that contain PII to those with a "need to know."

Limit storage of PII on shared drives and folders whenever possible.

Delete files containing PII and the SECNAV M-5210.1 Records Management Manual.

Verify that access controls are restored after maintenance.

DISCLOSURE OF PII. Disclosure of records pertaining to an individual from a system of records is prohibited except with his or her consent or as otherwise authorized by the Privacy Act, DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, or DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998. When DoD Components make such disclosures, the individual may, to the extent authorized by References (b) and (d), obtain a description of such disclosures from the Component concerned. Requests for such disclosures shall be referred to the NAVSUPPACT Naples Freedom of Information Act (FOIA) Coordinator. Individuals are permitted to (1) request access to records or to any information about themselves contained in a system of NAVSUPPACT Naples records; (2) obtain a copy of such records, in whole or in part; (3) correct or amend such records once it has been determined that the records are not accurate, relevant, timely, or complete; (4) appeal a denial for a request to access or a request to amend a record. Requests for such disclosures shall be referred to the NAVSUPPACT Naples Privacy Act Coordinator.

COMPLIANCE. All Department of the Navy personnel who handle PII must complete annual PII training, and the command must maintain auditable certificates of completion. All offices that handle PII must complete a Compliance Spot Check twice yearly, and the command must maintain auditable records.

REPORTING INCIDENTS. Contact your Privacy Act Coordinator (Staff Judge Advocate), the NAVSUPPACT Naples N1, or your immediate supervisor as soon as you suspect or have an actual loss or compromise of PII. If your PII is compromised, monitor financial accounts for suspicious activity. If your identity is stolen, immediately contact the Federal Trade Commission (FTC) for more information.

PRIVACY ACT. Due to the outstanding number of identity thefts that have affected the Department of Defense, The Secretary of the Navy mandated in reference that the use of SSN's of military members and civilian employees in routine correspondence was to be strictly limited. The only time that an exception is authorized is if the use of the number is essential for identification and authorized for use by authority of Executive Order 9397. The storage of documents that may contain full SSN's should be in a secure, controlled location such as a safe or, at the very minimum, a locked drawer. Work spaces should be sanitized at the end of a work day to ensure that no Privacy Act information is left out unattended. It is essential that this regulation be strictly adhered to in order to protect the identities of our service members and civilian employees.

PROTECTING PII IS EVERYONE'S RESPONSIBILITY

At a minimum, all NAVSUPPACT Naples personnel will be expected to do the following:

NAVSUPPACT NAPLES POLICY ON PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY ACT DATA (cont'd)

a. Take action to ensure that any PII contained in a system of records that you access and use to conduct official business will be protected so that the security and confidentiality of the information is preserved.

b. Not disclose any PII contained in any system of records, except as authorized by The Privacy Act, or other applicable statute, Executive order, regulation, or policies. Those willfully making any unlawful or unauthorized disclosure, knowing that disclosure is prohibited, may be subject to criminal penalties or administrative sanctions.

c. Report any unauthorized disclosures of PII from a system of records to your Privacy Act Coordinator.

d. Report the maintenance of any system of records not authorized by this directive to your Privacy Act Coordinator.

e. Minimize the collection of PII to that which is relevant and necessary to accomplish a purpose of NAVSUPPACT Naples.

f. Limit the availability of records containing PII to DoD personnel and DoD contractors who have a need to know in order to perform their duties.

g. Prohibit unlawful possession, collection, or disclosure of PII, whether or not it is within a system of records.

Safeguarding PII is everyone's responsibility. Make it your priority!

RANDAZZO.JOHN.LUCIAN.1035461376

Digitally signed by RANDAZZO.JOHN.LUCIAN.1035461376
Date: 2023.07.17 08:52:35 +02'00'

J. L. RANDAZZO