VA Network of Support (NoS) Pilot Privacy Policy Statement

NoS Pilot Privacy Policy

The authorization for the Department of Veterans Affairs (VA) to collect Personally Identifiable Information (PII) for the Network of Support (NoS) Pilot is derived from a legislative requirement (Public Law NO: 116-214, Section 101, Network of Support). In carrying out the NoS Pilot, the VA will use the NoS-related PII that you provide only for the following purposes:

- To link your NoS members to you,
- To communicate with you and your NoS,
- To send VA benefits information to your NoS,
- To confidentially use your demographic information on file for statistical analyses of NoS usage, and
- To send out a confidential survey for your feedback on NoS value and ease of use.

Your information will be stored, processed and protected according to VA policies and by law under the Privacy Act of 1974, 5 U.S.C. §522 and 38 U.S.C. §5701. Only authorized personnel with appropriate training will have access to your data. The VA will not disclose your personal information to third parties outside the VA without your consent or as authorized by law.

The privacy policies of NoS Pilot component systems are provided below.

_____

NoS Pilot Component Systems' Privacy Policies

In the NoS Pilot *startup phase*, two systems support the NoS Pilot. The NoS Processing System performs participant registration data collection, processing and storage, and the govDelivery platform provides distribution of VA benefits information to participants and direct email communications with participants for Pilot registration that utilizes a manual email-based process. The Privacy Policy Statements for the NoS Processing System and the govDelivery platform are in Sections 1 and 2 of this document.

In the Nos Pilot *mature phase*, three systems support the NoS Pilot: the IBM Get Results in Transition (GRIT) mobile application, the NoS Processing System, and govDelivery. The GRIT mobile platform provides participant registration functions through its Squad application, eliminating the need for the email-based manual registration process used at startup. The NoS Processing System continues to perform data collection, processing and storage functions, and the GovDelivery platform continues to provide distribution of VA benefits information to participants and email communications with participants for any registration functions that are not supported by GRIT. The GRIT Privacy Policy Statement is available in Section 3 of this document.

1. Privacy Policy for NoS Processing System

The NoS Processing System utilizes a Microsoft Access database for data storage coupled with software for data manipulation. In the startup phase, encrypted and password protected Microsoft Excel spreadsheets are used for manually collected registration information exchanges with the database. In the mature phase, a secure API is used for registration information exchanges between the database and GRIT. The system protects the data by leveraging password protection and encryption provided by Access, Excel and the secure API; and stores it in limited access file folders on the VA network. The data can only be seen by VBA privacy-trained NoS staff. The NoS Processing System generates mailing lists for use by govDelivery for email communication with participants, to monitor registration and communications status, and to analyze usage characteristics of NoS participants including transitioning service members (TSMs), Veterans, and their NoS members.

Type of Personal Information Collected and Analyzed in the NoS Interim Processing System
Contact Data. If you choose to participate in the NoS Pilot, the VA will use your contact information to communicate with your invited NoS members and you. The VA will store those contacts on its servers in the VA network.

How We Use Your Data
Your personal data will be used to communicate with you and your NoS and to anonymously analyze NoS usage.

Do We Share Your Personal Data with Third Parties?
Data stored, transformed, and analyzed by the NoS Interim Processing System is shared with GRIT and govDelivery for the purposes of communicating with you and your NoS members. Your data are not shared with third parties other than other U.S. Government authorities as permitted, necessary, or required by law. This may include disclosing your personal data to regulators, or law enforcement authorities. We may transfer and disclose the data we collect about you for the following reasons:

- To comply with a legal obligation, including, but not limited to, responding to a court order,
- To prevent fraud,
- To comply with an inquiry by a government agency or other regulator,
- To address security or technical issues, and
- To assist government entities in responding to an emergency.

How Do We Protect Your Data?
The VA is committed to ensuring that your personal data are secure. In order to prevent unauthorized access, loss or disclosure, we have put in place security controls that reduce the risks of a security breach of your personal data. Security controls include the use of encryption, multi-factor identification and need to know access, as well as the implementation of an extensive set of security controls as defined by the National Institute of Standards and Technology (NIST), VA, and other Federal Government security experts.

VA and contractor staff are required to follow VA PII privacy-related policies and procedures, and complete confidentiality training to understand the requirements of maintaining the confidentiality of customer information. All employees and contractors are required to complete privacy and security training.

2. Privacy Policy for Granicus govDelivery Platform

The NoS Pilot uses the Granicus govDelivery platform to send the VBA Newsletter to NoS Pilot participants, as well as to communicate with you and members of your NoS during the opt-in and opt-out process. govDelivery utilizes the email addresses and mobile phone numbers of you and your NoS, along with your name, for personalized communications with your NoS. You and your NoS's contact information is transferred from the NoS database to govDelivery as password-protected and encrypted files within the secure VBA network. Granicus will process your personal data in a transparent and lawful way. Any personal data will be used only in accordance with this privacy policy. For the complete Granicus privacy policy go to https://granicus.com/privacy-policy/.

Types of Personal Information Collected
Contact Data. If you choose to participate in the NoS Pilot, govDelivery will use your contact information to communicate with your invited NoS members and you. Granicus will store those contacts on its servers.

How govDelivery Uses Your Data
Your data will be used to communicate with you and your NoS or for other legitimate interests such as:

- Providing high-quality customer service.
- Complying with laws or regulations that apply to us.
- Developing the govDelivery suite of products, our websites and other products and services

- Developing and improving the network security, efficiency and technical specification of our IT systems and infrastructure.

Do We Share Your Personal Data with Third Parties?
Granicus will share your personal data as permitted, necessary, or required by law. This may include disclosing your personal data to regulators or law enforcement authorities only for the following reasons:

- To comply with a legal obligation, including, but not limited to responding to a court order.
- To prevent fraud.
- To comply with an inquiry by a government agency or other regulator.
- To address security or technical issues.
- To assist government entities in responding to an emergency.
- As part of a business transaction.

If the ownership of Granicus changes, or if it merges with or is acquired by another organization, or if it liquidates its assets, your personal data may be transferred to the new organization. If this occurs, the successor organization's use of your data will still be subject to this policy and the privacy preferences you have expressed to us.

Do We Sell Your Data to Others?
No. Granicus does not buy or sell personal data.

How Do We Protect Your Data?
Granicus is committed to ensuring that your personal data are secure. In order to prevent unauthorized access, loss or disclosure, the company has put in place security controls that reduce the risks of a security breach of your personal data.

Your information will be stored and processed within the secure VA network protected according to VA policies and by law under the Privacy Act of 1974, 5 U.S.C. §522 and 38 U.S.C. §5701. Employees and contractors are required to follow policies, procedures, and complete confidentiality training to understand the requirement of maintaining the confidentiality of customer information. All employees are required to complete privacy and security training.

Policies and Practices for Retention, Disposal, and Contesting of Records
To exercise any of the following, please contact support@granicus.com. Under certain circumstances, by law you have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data held about you and to check that it is being lawfully processed.
- Request correction or completion of the personal data held about you. This enables you to have any incomplete or inaccurate information held about you corrected.
- Request the portability of your data to another provider (only where Granicus is relying on consent or contractual necessity).
- Request erasure of your personal data. This enables you to ask to have your personal data deleted or removed when there no longer is good reason for Granicus to continue processing it.
- Request objection to processing of your personal data. This enables you to object to processing of your personal data even when Granicus is relying on a legitimate interest.
- Request the restriction of processing of your personal data. This enables you to ask Granicus to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.

- Withdraw your consent to the processing of certain personal data (only where you have previously provided consent).
- Make a complaint. You can make a complaint about govDelivery privacy practices at any time to the Granicus Corporation (Granicus, LLC and Granicus-Firmstep, Ltd.) by mail: 408 St. Peter Street, Suite 600, St. Paul, MN 55102; or by phone: 01 651 400 8730; or by email: support@granicus.com.

Granicus may need to request specific information from you to help it confirm your identity and ensure your rights to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data are not disclosed to any person who has no right to receive it.

3. Privacy Policy for IBM Get Results in Transition (GRIT) Mobile Application

GRIT's Squad function will be used by the NoS Pilot as the registry for NoS participants (TSMs, Veterans, and their selected friends/family members). If you elect to become a NoS Pilot participant, you will be asked to opt-in and provide your name, email address, and mobile phone number using the Squad function in GRIT. TSMs and Veterans will also be asked to provide their Department of Defense ID during registration. The GRIT application has support capabilities besides Squad that TSMs and Veterans may use at their discretion; but only the Squad function is used directly as part of the NoS Pilot.

If you are a NoS Pilot participant and opt in using GRIT Squad, the complete IBM GRIT Privacy Policy can be found at: https://www.gritforvets.org/privacy.html.