GovLoop Privacy Policy

Last updated: February 1, 2024

1. Overview

Your information will be held by Granicus, LLC ("Granicus"). GovLoop, ("GovLoop", "Company", or "We"), which is a division of Granicus, operates within its own value streams and markets, and is committed to maintaining your trust by protecting your personal data. This statement explains how we collect, use, share and protect your personal data. Personal data is any information relating to an identified or identifiable person. Your name, address, phone number, bank account number, email address and your IP address are examples of personal data. Unless otherwise specified, this notice applies to GovLoop's marketing efforts.

GovLoop will process your personal data in a transparent and lawful way. Any personal data you provide when using this website or our products and services will be used only in accordance with this privacy statement.

Granicus complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. Granicus has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF.

If there is any conflict between the terms in this privacy policy and the Data Privacy Framework Principles, the Data Privacy Framework Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/. For further information regarding our participation in the Data Privacy Framework, please see Sections 9 and 10 below.

The Granicus entities which adhere to this Privacy Notice and the DPF Principles are GovLoop and, Granicus, LLC, including all U.S. entities and U.S. subsidiaries using the brand name Granicus.

We may change this statement from time to time to reflect privacy or security updates. If we make material changes, we will notify you via the email address listed in your account or by means of a notice on this website prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

This privacy statement is provided in a layered format so you can click through to the specific sections set out below.

2. How Can You Contact Us?

In compliance with the EU-U.S. DPF, amd the UK Extension to the EU-U.S. DPF, Granicus commits to resolve DPF Principles-related complaints about our collection and use of your personal information. If you have questions about this statement or if you would like to exercise any rights you may have in relation to your personal data, please contact us at info@govloop.com. If you have additional questions or need to escalate an issue, use the below details to contact our Data Protection Officer (DPO):

Full name of legal entity: Granicus, LLC, as described above
Name of DPO: Data Protection Officer
Email address: dpo@granicus.com
Postal address: 1152 15th Street NW, Suite 800, Washington, DC 20005, USA
Telephone number: 01-651-400-8730

3. What Personal Data Does GovLoop Collect, and for What Purpose?

We may collect your personal data such as your name, place of employment and address, job position, e-mail address, and phone number. This data is collected directly from you through forms on our website or over the phone and is used to communicate and personalize such communications with you, including offering products and services that we believe may be of interest to you.

Information about your chosen subscriptions is used to better provide you with relevant e-mail content. We may also gather data about you from referrals from existing community members. In certain situations, such as when you authorize a social network to prefill a form on our website or if you interact with social media buttons on our website, we may receive publicly available information from your social media profile (such as first name, last name, e-mail address, date of birth, gender, job title, and company).

In order to provide you with free resources, online trainings, and events, GovLoop may share your data with online training, event or resource underwriters. When you register for an online training/event or download a resource, your information may be shared with the sponsors of that document or training. You have the option to unsubscribe or opt-out from sponsor communications with said sponsor at any time.

We also gather certain data automatically upon your visit to our website, including Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, the files viewed on our site and e-mails (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data to analyze trends in the aggregate and administer the site. Your IP address may also be utilized to infer your location, which we may use to send you more relevant content.

We will not collect additional categories of personal information or use the personal information we collect for materially different, unrelated, or incompatible purposes without providing you notice.

In the preceding twelve (12) months, we have collected, disclosed or sold the following categories of personal information:

Category	Examples	Collected (YES/NO)	Shared (YES/NO)	Sold (YES/NO)
A. Identifiers.	First Name Last Name Email Address Job Title Organization Business Phone Number Address State City Zip Country Job Function Type of Government Mobile Phone Number (this is not shared or sold) IP address (this is not shared or sold)	YES	YES	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	Name, address, telephone number, credit card number, debit card number, username or email address in combination with a password. Some personal information included in this category may overlap with other categories.	YES	NO	NO
C. Internet or other similar network activity.	Browser type, Internet service provider (ISP), operating system, date/time stamp	YES	NO	NO
D. Digital Behavior	Referring/exit pages, the files viewed on our site and e-mails (e.g., HTML pages, graphics, etc.), clickstream	YES	YES	YES
E. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO	NO	NO
F. Commercial information.	Records of personal property, products or	NO	NO	NO

	services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.			
G. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO	NO	NO
H. Geolocation data.	Physical location or movements.	NO	NO	NO
I. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO	NO	NO
J. Professional or employment-related information.	Current or past job history or performance evaluations.	NO	NO	NO
K. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO	NO	NO
L. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO	NO	NO

4. How Do We Justify Collecting Your Data?

We will use your personal data when the law allows us to. Most commonly, for marketing purposes, we will process your personal data in the following circumstances:

- Where you consent; or

- Where it is necessary for our legitimate interests (i.e. we have a business or commercial reason for using your information) and your interests and your fundamental rights do not override those interests.

When applicable, our legitimate interests may include:

- Providing high-quality customer service.
- Complying with laws or regulations that apply to us.
- Developing our products and services, and what we charge for them.
- Defining customers for our products and services.
- Seeking your consent when we need it to contact you.
- Providing our customers with relevant marketing, and other high-quality product and service features.
- Keeping our marketing updated and relevant.

5. What Happens If We Process Your Data for Other Purposes?

We will only use your personal data for the uses and purposes set out above, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original uses and purposes. If we need to use your personal data for an unrelated purpose, we will notify you and will explain the legal basis which allows us to do so.

6. What Happens If You Do Not Provide The Data?

Where we need to collect personal data by law or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with resources or services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

7. Do We Use Algorithms To Make Decisions About You?

We will not use your personal data for decisions based solely on automated processing if the decision has legal effects concerning you or if it significantly affects you, unless you gave your explicit consent for this processing.

8. Do We Share Your Personal Data with Third Parties?

We share your personal data with the following categories of recipient:

- Agents and subcontractors. We may disclose your personal data with our agents or subcontractors for the purposes identified above. In these cases, the agent or subcontractor will be obligated to use that personal data in accordance with the terms of this privacy statement. Your data may be shared with these types of agents and subcontractors.
    - Marketing automation and analytics service provider
    - Transactional email service provider
    - Opt-in tool provider

- Webinar hosting platform
- Advertising platform

- Government authorities as permitted 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; or
  - To assist government entities in responding to an emergency

- As part of a business transaction. In relation to an ongoing or proposed business transaction such as a transfer of the ownership or operation of Granicus, LLC or any companies in its group to another organization, if we merge with or are acquired by another organization, or if we liquidate our assets, your personal data may be transferred to a successor organization. If such a transfer occurs, the successor organization's use of your data will still be subject to this statement and the privacy preferences you have expressed to us.

We share your personal data with the following categories of recipient and such sharing constitutes a "sale" under the California Consumer Privacy Act.

- Sponsors. We may disclose your personal data with our sponsors. Our sponsors generally underwrite resources and online training so that we may provide these resources at no cost to you. Sponsors are typically solution providers or consulting services who operate independently of GovLoop. They are disclosed by including their logos on their respective underwritten/sponsored content or on the landing page where you submit your information to register or download said resource. We may not share your data in all cases when downloading or registering for a sponsored resource.

  You can opt-out of communications with these sponsors at any time through that sponsor's unsubscribe mechanisms.

9. Do We Participate in the Data Privacy Framework?

Yes. Granicus complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF)and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/ and search for "Granicus".

We are responsible for the processing of personal data we receive or subsequently transfer to a third party acting as an agent on our behalf. We will comply with the Data Privacy Framework Principles for all onward transfers of personal data from the EU and the UK, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to Data Privacy Framework, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In addition, Granicus commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO),the Gibraltar Regulatory Authority (GRA) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, and the UK Extension to the EU-U.S. DPF. You may engage such authorities if you have concerns regarding our adherence to the Data Privacy Framework Principles or any applicable privacy law or regulations. We will respond directly to such authorities regarding investigations and resolution of complaints. Under certain conditions, more fully described on the Data Privacy Framework website, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted. For more information on this option, please see Annex I of the EU-U.S. Data Privacy Framework Principles.

10. Where Does Your Data Go?

GovLoop is owned and operated within the United States. Therefore, the data that we collect from you will be transferred to, and stored at, a destination outside the European Economic Area ("EEA")/UK.

Granicus' compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), and the UK Extension to the EU-U.S. DPF deems the organization to provide adequate privacy protection, which is a requirement for the transfer of personal data outside of the European Union under the EU General Data Protection Regulation (GDPR), and outside of the United Kingdom under the UK Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

11. How Do We Protect Your Data?

We are committed to ensuring that your personal data is secure. To prevent unauthorized access or disclosure, we have put appropriate technical and organizational measures in place to safeguard and secure your personal data.

If a data breach does occur, we will do everything in our power to limit the damage. In case of a high-risk data breach, and depending on the circumstances, we will inform you about remedial actions to prevent any further damage. We will also inform the relevant supervisory authority or authorities of the breach.

Unfortunately, no security measures are completely secure. We, therefore, cannot guarantee that your personal data will not be disclosed, misused or lost by accident or by the unauthorized acts of others. Further, we cannot control the dissemination of personal data you post in the public domain and you should have no expectation of privacy in respect of such data.

The procedures and related standards include limiting access to data and regularly testing and auditing our security practices and technologies.

Employees and temporary workers are required to follow policies and procedures and complete confidentiality training to understand the requirement of maintaining the confidentiality of customer information. If they fail to do so, they are subject to disciplinary action. All employees are required to complete privacy, security, ethics and compliance training. We also offer a wide variety of other training to all employees and temporary workers to help us achieve our goal of protecting your personal data.

12. How Long Will We Keep Your Data?

We retain your personal data for as long as your account is still open. We retain the personal data you provide while your account is in existence or as needed to provide you services. Even if you only use our services every few years, we will retain your information and keep your profile open until you decide to close your account. However, it may not always be possible to completely remove or delete all your personal data from our databases without some residual data because of backups and other reasons.

To determine the appropriate retention period for the information we collect from you, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of the data, the purposes for which we process the data, whether we can achieve those purposes through other means, and the applicable legal requirements.

13. What Rights Do You have?

To exercise any of the following rights, please contact info@govloop.com. If you need to escalate a matter or feel that your issue is unresolved, please contact our DPO. You may also exercise some of these rights (such as access and edit your information, or delete your profile) by visiting GovLoop's website : https://www.govloop.com/members/{your username}/

Removing your profile/account from GovLoop.com does not delete your data from our marketing database. If you wish to remove this data, send a request to info@govloop.com.

You have the option to unsubscribe or opt-out from any sponsor communications with said sponsor at any time. You can also update your email subscription preferences with GovLoop at any time: https://go.govloop.com/EmailPreferences.html

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month for particularly complex requests or if you have made several requests. In this case, we will notify you and keep you updated.

13.1 Right to Request Access

You have the right to request details of your personal data that we hold, including the categories of personal data collected, the sources from which it was collected, the purpose for such collection, the categories of third parties with whom such data is shared, and the specific data collected. Upon request, we will provide a copy of such personal data within a reasonable timeframe.

13.2 Right to Rectification

If you believe that any personal data we are holding on you is incorrect or incomplete, please contact us as soon as possible, at the address above. We will promptly correct any personal data found to be incorrect, though we may need to verify the accuracy of the new data you provide to us.

13.3 Right to Object

You may choose to object to the processing of your personal data where we are relying on a legitimate interest and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your data which override your rights and freedoms. You also have the right to object in cases where we are processing your personal data for direct marketing purposes. We will provide you with appropriate choices to opt-in or opt-out as set out above in this statement.

Please note that your objection may be overridden by the legitimate interests of GovLoop to process and collect your personal data.

13.4 Right to Erasure

To the extent legally permissible, you may be entitled to have certain personal data erased in the following circumstances:

1. The personal data is no longer necessary in relation to the purposes for which it was collected or processed.
2. You object to the collection or use of your personal data and there are no overriding legitimate grounds for the processing.
3. The personal data has been unlawfully processed.
4. The personal data has reached the defined retention period or for compliance with a legal obligation to which GovLoop is subject.

Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

13.5 Right to Restriction of Processing

You may have the right to restrict further processing of your personal data in the following situations:

1. You contest the accuracy of the personal data.
2. The processing of the data is unlawful.
3. The personal data has reached the defined retention period, but you require the personal data to establish, exercise, or defend legal claims.
4. You object to the processing of data pursuant to the right to object as described above. The processing may be restricted pending the verification of whether GovLoop's legitimate grounds override your rights as a data subject.

13.6 Right to Portability

You have the right to receive your personal data in a structured, commonly used and machine-readable format. GovLoop will assist in the transmission of such data to another entity, upon request, to the extent technically feasible. Note that this right only applies to automated information which you initially provided consent for us to use, or where we need the info to perform a contract with you.

13.7 Right to Revoke Consent

If you have consented to the processing of your personal data via the explicit checkbox located on forms on landing pages, you have the right to revoke such consent by emailing info@govloop.com at any time. The checkbox will only appear for individuals who reside in countries within the EU/UK. Individuals from any country can request to delete their data the same way – by emailing info@govloop.com. However, if you withdraw your consent, this will not affect the lawfulness of any processing carried out before you withdraw your consent.

13.8 Right to Make a Complaint

You have the right to make a complaint at any time to the relevant local, national or industry privacy regulator. We would, however, appreciate the chance to deal with your concerns before you approach your supervisory authority so please contact us in the first instance.

13.9 Right to Opt-Out of Data Sale

For residents of California, you have the right to direct us to not sell your personal information. You may do so by accessing our CCPA portal.

14. Will We Penalize You for Using Your Rights?

We will not discriminate against you for exercising any of your rights under applicable law (such as GDPR, CCPA etc.). Unless permitted by applicable law, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.

- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

15. Do We Track You Online?

GovLoop and its partners use cookies or similar technologies to analyze trends, administer the website, track users' movements around the website, and to gather demographic information about our user base. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our website or service.

We also partner with third parties to display advertising on our website or to manage our advertising on other sites. Our third-party partner may use cookies or similar technologies in order to provide you advertising based upon your browsing activities and interests. If you are in the UK, European Union or California you will be provided with a cookie notice when you visit the site. The cookie notice will provide you an option to update your preference. In the alternative, you may click here [or if located in the European Union click here] to opt-out of interest-based advertising. Please note you will continue to receive generic ads.

Currently, various browsers offer a "do not track" or "DNT" option and global privacy control which sends a signal to websites visited by the user about the user's browser DNT preference setting. We will do our best to respect such signals we receive, and notify you as required when placing tracking technologies on your device.