

GDPR – Annotated Privacy Statement

Granicus

September 6, 2018

Version 1.1

Introduction:

Granicus LLC. and GovDelivery Europe, Ltd. (“Granicus” or “Company”) is committed to maintaining your trust by protecting your personal data. This Privacy Statement explains our practices for the collection, use, and other processing of your personal data (as described in more detail below).

Granicus is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this Privacy Statement.

Granicus is committed to ensuring that your privacy is protected. Granicus shall process your personal data in accordance to the terms of this Privacy Statement.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

In furtherance of the Company’s commitment to this Policy, Granicus, LLC has certified to adhere to the Privacy Principles set forth in the US-EU Privacy Shield Framework (alternatively, “Accord”) regarding Personal Data related to candidates resident in the European Economic Area (“EEA”) and processed in support of Company human resources operations. Company adheres to the Privacy Shield principles as respectively agreed to by the U.S. Department of Commerce and the European Commission. With respect to Personal Information received or transferred pursuant to Privacy Shield, Granicus, LLC is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. Granicus, LLC’s commitment to participate in the Privacy Shield program can be found at the following DOC website located at <https://www.privacyshield.gov> that officially lists all U.S. entities that have registered for the program. Granicus has further committed to cooperate with EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU.

This is the latest version of this Privacy Statement. Nothing in this Privacy Statement shall be deemed to constitute a contract of employment nor shall it form part of any potential subsequent contract of employment you may be given. Granicus may amend this Privacy Statement from time to time by updating this page.

What is personal data?

Personal data is any information relating to an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are “special categories” of more sensitive data which require a higher level of protection. These “special categories” of data include: information about your ethnicity, religious beliefs, sexual orientation and political opinions, information about your health, including any medical condition and health and sickness records.

1. Which personal data do we process for which purposes?

We will only use your personal data when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to comply with a legal obligation.
2. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest.

Personal Data Type (with examples)	Collection Purposes
Personal Identification: -Name -Date of birth -Gender -Nationality -Race or ethnic origins	Legal Obligations: To comply with applicable laws, including immigration requirements. Legitimate interest(s): To conduct the recruitment process and ensure meaningful equal opportunities monitoring and reporting.
Contact Information: -Home address -Telephone number -Email	Legitimate interest(s): To communicate with you as part of the recruitment process.
Recruitment Data: -Work History -Education History -Academic and professional qualifications -Applicant Assessment Results -Interview notes -Professional References -Details of disabilities or medical conditions	Legitimate interest(s): To conduct the recruitment process. Legal Obligations: To comply with applicable laws, including in relation to health and safety and disability discrimination.

If you fail to provide certain information when requested, we may not be able to progress your application, or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

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

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

2. How do we use particularly sensitive personal information?

As mentioned above, "special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with your potential future employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will use your particularly sensitive personal information in the following ways:

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We may use information about your race or ethnic origins to ensure meaningful equal opportunities monitoring and reporting.

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of the recruitment process that you agree to any request for consent from us.

3. Automated decision-making

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

4. International Data Transfers

As a global company, Granicus employs a multifaceted approach to protecting personal information. For example, when transferring personal information between corporate entities, Granicus relies on different legal transfer mechanisms (e.g., standard contractual clauses or Privacy Shield certification) depending on the type of personal information needed and countries involved. Please contact [Granicus] [our Data Protection Officer (dpo@granicus)] for any questions you might have or for additional information regarding the protections in place to protect your personal information.

5. Do we share your personal data with third parties?

We may disclose your personal data to our agents or sub-contractors, such as our applicant tracking system vendor, for the purposes identified above. In such cases, the agent or sub-contractor will be obligated to use that personal data in accordance with the terms of this Privacy Statement.

We will not sell, distribute or lease your personal data to third parties unless we have your permission or are required by law to do so.

We may disclose your personal data without your permission to the extent that it is required to do so by applicable law, including in connection with any legal proceedings or prospective legal proceedings, and in order to establish, exercise or defend our legal rights.

We disclose your personal information to our private equity sponsor, Vista Equity Partners, and its affiliates, including Vista Consulting Group (collectively, "Vista"), for administration, research, database development and business operation purposes, in line with the terms of this Privacy Policy. Vista processes your personal information on the basis of its legitimate interests in overseeing the recruitment process and, if applicable, your employment relationship with Granicus. If you have consented to us doing so, we also share your personal information with other Vista portfolio companies for the purpose of being considered for other job opportunities in the pooling system, both inside and outside the EEA. Please find a full list of all Vista portfolio companies at: <https://www.vistaequitypartners.com/companies/>. Where this requires us to transfer your personal information outside of the EEA, please refer to Section 4 of the Privacy Policy for further details on cross-border transfers. In connection with the recruitment process, we transfer your personal data outside of the EEA to Hirebridge, LLC and Criteria Corp., which provide applicant tracking services. Hirebridge, LLC and Criteria Corp. both comply with the EU-U.S. Privacy Shield Framework and ensure that your personal information is adequately protected whilst outside of the EEA

Prior to disclosing personal data to a third party beyond our legal obligations, or otherwise stated herein, the Company shall notify you of such disclosure and ask for your express consent to opt-into such disclosure. Granicus shall enter into contracts with any third party to whom personal data may be disclosed so that such parties are aware of and adhere to the Privacy Shield Principles and the data protection requirements of any applicable privacy law or regulation such as the General Data Protection Regulation ("GDPR"), as applicable. The Company shall also, upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing by third party agents and agrees to provide a summary or a representative copy of the relevant privacy provisions of its contracts with agents of the DOC upon request.

Granicus shall ensure by contract that any third party vendor (a) complies with the Privacy Shield Principles and (b) the data protection requirements of any applicable privacy law or regulation such as the GDPR and (c) has contractual safeguards in place to protect the personal data.

Granicus is responsible for the processing of personal data it receives, under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Granicus complies with the Privacy Shield Principles for all onward transfers of personal data from the EU, including the onward transfer liability provisions.

6. Security

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

7. Data retention

We will store your personal data for no longer than is necessary for the performance of our obligations or to achieve the purposes for which the information is collected, or as may be permitted under applicable data protection laws.

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

When we no longer need to use your personal data, we will remove it from our systems and records or take appropriate steps to properly anonymize it so that individuals can no longer be identified from it (unless we need to keep your personal data to comply with legal or regulatory obligations).

8. Data subject rights

To exercise any of the following rights, please contact recruitment@granicus.com.

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party in a structured, commonly used and machine-readable format and Granicus will assist in the transmission of such data to the extent technically feasible.
- **Revoke consent** to the processing of certain personal information to which you have previously provided consent.

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

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

9. Recourse, Reinforcement, and Liability

Granicus periodically verifies that the policy is accurate, comprehensive for the information intended to be covered, is disseminated to its employees, is completely implemented and accessible and is in conformity with the Privacy Shield Principles set forth in this Policy. Granicus encourages interested persons to raise any concerns using the contact information provided herein and will investigate and attempt to resolve any complaints and disputes regarding use and disclosure of personal data in accordance with the Privacy Shield Principles. In addition, Granicus has agreed to cooperate with the **European Data Protection Authorities** [http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm] for the purpose of handling any unresolved complaints regarding Personal Data concerns. Data Subjects may engage their local Data Protection and/or Labor Authority concerning adherence to the Privacy Shield Principles and any applicable privacy law or regulation and the Company shall respond directly to such authorities with regard to investigations and resolution of complaints. Under certain conditions, more fully described on the Privacy Shield website [<https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>], you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

10. Further information

If you have any questions about this Privacy Statement or questions or complaints about the processing of your personal data by Granicus, please contact:

Carrie Cisek, VP of Human Resources
408 St. Peter Street, Suite 600
St. Paul, MN 55102, USA
01 651 757 4114
hr@granicus.com

If using the contact information above does not sufficiently resolve your complaint, residents in designated countries may also have the right to contact our Data Protection Officer

Gerry Hansen, Data Protection Officer
408 St. Peter Street, Suite 600
St. Paul, MN 55102, USA

01 651 925 5765
dpo@granicus.com