Granicus GDPR/ CCPA Candidate Privacy Policy

Last Updated: March 30, 2021

Version 2.1

1. OVERVIEW

Granicus LLC. and Granicus-Firmstep, Ltd. ("Granicus" or "Company") is committed to maintaining your trust by protecting your personal data. This Privacy Policy explains our practices for the collection, use, and other processing of candidate personal data.

Granicus is a "data controller". This means that we are responsible for deciding how we hold and use personal data about you.

This is the latest version of this Privacy Policy. Nothing in this Privacy Policy 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 Policy from time to time by updating this page.

2. HOW CAN YOU CONTACT US?

If you have any questions about this Privacy Policy or questions/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, you can also contact our Data Protection Officer or our EU representative:

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

01 651-400-8730
dpo@granicus.com

Name of EU representative: DataRep
Email address: granicus@datarep.com
You can also contact DataRep using this online form: https://www.datarep.com/data-request
Postal address: The Cube, Monahan Road, Cork, T12 H1XY, Republic of Ireland

3. WHAT PERSONAL DATA DOES GRANICUS COLLECT, AND FOR WHAT PURPOSES?

As a candidate for employment with Granicus, we have to collect some information. Normally, you will supply us with this information via a Curriculum Vitae or Resume, or through an online form while applying for a job. Personal data will include name, contact details, work and education history, professional references, interview notes, assessment results, work authorization, and VISA sponsorship details.

This data is collected as a pre-condition to entering into a contract with Granicus and we will use it only for the purposes of evaluation and selection of the most appropriate candidates for interview, and then for entering into an employment contract with successful candidates.

In addition, we may collect details on race or ethnic origins, and disabilities or medical conditions to fulfil any legal obligations we have, or in order to make reasonable adjustments to facilitate your interview experience. 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.

4. HOW DO WE USE PARTICULARLY SENSITIVE PERSONAL DATA?

Some data is known as "special category data". This is particularly sensitive personal data that requires higher levels of protection.

We will use information about your physical or mental health, or disability status to ensure your health and safety in the workplace, to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence, and to administer benefits if hired.

We will use information about your race or ethnic origins to ensure meaningful equal opportunities monitoring and reporting.

This information is collected where necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment.

5. WILL COMPUTERS OR PEOPLE MAKE THE DECISIONS?

We may use automated systems that select candidates based on certain criteria we decide. If we do so, we will set out the logic behind that decision-making process and give you the right to have that decision re-evaluated by a human being. This may include candidate testing as part of the interview process, but we will ensure a human is involved in any decision-making process.

6. DO WE SHARE YOUR PERSONAL DATA WITH THIRD PARTIES?

Yes. We may disclose your personal data to the following agents or sub-contractors for the purposes identified above:

- Applicant tracking system vendor
- Assessment provider
- Background check service provider

In such cases, the agent or sub-contractor will be obligated to use that personal data in accordance with the terms of this Privacy Policy, and we will have a contract that obligates them to similar levels of protection.

We may also 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 data 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 data on the basis of its legitimate interests in overseeing the recruitment process and, if applicable, your employment relationship with Granicus.

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.

7. DO WE PARTICIPATE IN PRIVACY SHIELD?

Yes. We have certified to adhere to the Privacy Principles set forth in the US-EU Privacy Shield Framework regarding the collection, use, and retention of personal data transferred from the European Union ("EU") and the United Kingdom ("UK") to the United States. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

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 Privacy Shield 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 Privacy Shield, 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, we will cooperate with the European Data Protection Authorities for any unresolved complaints regarding personal data. You may engage your local Data Protection and/or Labor Authority if you have concern regarding our adherence to the Privacy Shield 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 Privacy Shield website, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

8. WHERE WILL YOUR DATA BE HELD?

Granicus 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.

In light of the July 16, 2020 "Schrems II" decisions, the European Court of Justice has decided that the EU-US Privacy Shield is no longer a valid international data transfer option. We plan to maintain our Privacy Shield certification as good practice; however, we will no longer rely upon it as a basis for data transfer. We will discuss with any partner relying on it for EU-US transfers their proposed alternative solutions.

The remaining option open to us for data transfers are Standard Contract Clauses (SCCs) and we are therefore engaging with our partners to:

1) Review all our data transfers globally to identify areas that require change,
2) Switch Privacy Shield transfers to EU approved Standard Contract Clauses as a default, and
3) Introduce additional contractual, organizational and technical safeguards to further protect your information.

Likewise, we are aware of the UK's exit from the EU and the end of the current transition period on December 31st, 2020. We will follow the new UK Information Commissioner's Office (ICO) and the European Data Protection Board (EDPB) guidance on data transfer when it becomes available.

We will continue to rely on legal derogations for case-by-case transfers where appropriate and will identify where this is the case.

9. HOW DO WE PROTECT YOUR DATA?

We are committed to ensuring that your personal data is 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. We will ensure our partners and subcontractors do the same.

10. HOW LONG WILL WE KEEP THE PERSONAL DATA?

We will store your personal data for no longer than we need it for the recruitment process, or how long we are legally required to hold it. We will retain the data for a period of eighteen months after the recruitment process has concluded in the case you have an enquiry about your application. If you are offered and accept employment, your data will be retained in line with the Employee Privacy Policy.

During the recruitment process we will ask you if you wish for your data to be retained for a further period in order to be considered for other positions that may be relevant to you. If you have consented to us doing so, we will share your personal data with other Vista portfolio companies for the purpose of being considered for other job opportunities in the pooling system, both inside and outside the European Economic Area (EEA). Please find a full list of all Vista portfolio companies at: https://www.vistaequitypartners.com/companies/.

When we no longer need to use your personal data, we will either 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 any legal or regulatory obligations).

11. WHAT RIGHTS DO YOU HAVE?

To exercise any of the following rights, please contact recruitingteam@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 we hold about you and to check that we are lawfully processing it.
- Request correction or completion of the personal data 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 data. This enables you to ask us to delete or remove personal data if we no longer have good reason for continuing to process it.
- Request the restriction of processing of your personal data. This enables you to ask us 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.
- Request your rights in relation to automated processing of your data, such as a description of the logic and human involvement.
- Withdraw your consent to the processing of certain personal data (only where you have previously provided consent).
- Right to withdraw your candidacy at any time.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the data (or to exercise any of your other rights). This is

another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

12. WHAT IF YOU NEED TO MAKE A COMPLAINT?

We hope you won't need to! However, if you do have any concerns, please get in touch by contacting recruitingteam@granicus.com.

You have the right to make a complaint at any time to the relevant data protection supervisory authority in the EU member state in which you reside.

13. WHAT IF YOU ARE A CALIFORNIA RESIDENT?

Congratulations, the CCPA (California Consumer Privacy Act) will apply to your data!

The CCPA covers the last 12 months of data, and includes rights such as access, deletion, opt out of sale, etc. But don't worry, we endeavor to treat all of our staff the same and we will try to give you other GDPR rights that we mention in this policy! Some national and state timescales are different, and we'll notify you of them if you want to use those rights. In addition, you can bring your complaints to a regulator, in this case the California Attorney General.

Importantly, the CCPA requires us to notify you if we buy or sell your data for any benefit. We do not buy or sell candidate data; data is collected directly from you.

We collect the same category of data irrespective of your location (whether you reside in the EU or California) and for the same purpose. The collected data is shared only with the third parties mentioned in section #6 of this policy.