Granicus GDPR/ CCPA Employee Privacy Policy

Last Updated: October 19, 2022

Version 3.0

1. OVERVIEW

Granicus LLC ("Granicus" or "Company") is committed to maintaining your trust by protecting your personal data. This Privacy Policy is drafted based on local laws and legislation that considers our mutual rights and explains our practices for the collection, use, and other processing of employee 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.

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 an employee of Granicus, we must collect some information. Normally, you will supply us with a Curriculum Vitae or Resume when you begin employment, and we will collect further information during your employment, such as when you apply for a training course, update us about a change to your circumstances, or when monitoring your performance, etc.

Categories of personal data that Granicus will process include:

- Identification data such as name, gender, date of birth
- Contact details such as phone, address, email, emergency contact details
- National identifiers such as national insurance number, passport, driving license, social security number, immigration and visa status
- Spouse, beneficiary & dependents information, marital status, or veteran status where required
- Compensation and benefit information such as salary, pension, benefits elections
- Payroll information such as banking details, tax information
- Health information including any disabilities, medical conditions, or sickness records where locally required
- Employment details such as employee agreement/contracts, performance reviews, disciplinary/grievance records, training information, absence records
- Information provided during the recruitment process
- Race or ethnicity details
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organization; you will be notified separately if this is to occur)
-
- Criminal records information, including the results of Disclosure and Barring Service (DBS) checks

- IT information— information about your use of our IT, communication and other systems, and other monitoring information. Information required to provide access to company IT systems and networks such as IP addresses, log files, login information, software/hardware inventories
- Your image, in photographic and video form

You will provide some of this information to us through various information collection forms and software applications; others are collected during your employment activities, such as when you log on to our IT systems.

We will use your personal data for the following purposes:

- Staff administration
- Employment contracts
- Providing staff benefits
- Exercising legal rights
- Performance management and training
- Expense management
- Employee recognition
- Employee engagement survey
- Monitoring the use of IT systems

This information is necessary for the employment contract with Granicus, to fulfil legal obligations we have, to protect your health or wellbeing, or where it is in our legitimate interests to do so without encroaching on your privacy rights.

We will try and give you choices where possible, but in most cases if you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

We may collect this information from you, your manager, your personnel records, the Home Office, pension administrators, your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators, the DBS, other employees, consultants and other professionals we may engage, e.g. to advise us generally and/or in relation to any grievance, conduct appraisal or performance review procedure, door entry systems, swipe card systems, application logs, keystrokes and mouse movements, screen capture, application logs, webcams, automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, remote

access systems, email and instant messaging systems, intranet and Internet facilities, telephones, voicemail, mobile phone records data loss prevention tools, next-generation firewalls, unified threat management systems, transport layer security, eDiscovery technology, mobile device management systems, relevant websites and applications.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or to the purposes for which we collect and process it.

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, comply with employment laws, to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence, and to administer benefits.
- Where locally required, we may use information about your race, national or ethnic origin, religious, or your sexual orientation, to ensure meaningful equal opportunity 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 identify behaviors and activities based on certain criteria we decide, such as monitoring the use of our IT networks, or selecting employees with skills. 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.

Likewise, we are aware of the UK's exit from the European Union and the end of the current transition period on December 31st, 2020. We are aware that the UK hopes for a positive adequacy decision from the EU by then to allow data transfers to continue, but we will continue to monitor the situation in case alternative transfer mechanisms from EU to UK or UK to US become available or necessary.

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

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

Yes. We may disclose your personal data to our agents or sub-contractors for the purposes identified above. In such cases, the agent or sub-contractor will be obligated to use the personal data in ways consistent with the terms of this Privacy Policy, and we will have a contract that obligates them to similar levels of protection. Your data may be share with these types of agents and sub-contractors:

- Human Resources Information System (HRIS) service provider
- Compensation management system provider
- Payroll processor
- Benefits provider/ broker/administrator
- Assessment distributor
- Employee survey or engagement software provider
- Employee recognition platform provider
- Expense management service provider
- eSignature platform provider

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 based on its legitimate interests in overseeing the recruitment process and 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. WHERE WILL YOUR DATA BE HELD?

Information may be held at our offices and those of our group companies, and third-party agencies, service providers, representatives and agents as described above. Information may be transferred internationally to the USA and other countries around the world, including countries that do not have data protection laws equivalent to those in

the EU/UK. To ensure compliance with EU/UK data protection legislation, we have entered into an Intra-Company Group Data Transfer Agreement that has adopted the EU Standard Contractual Clauses as a mechanism to ensure the adequate safeguard of your personal information when transferred outside the EU/UK. We have security measures in place to seek to ensure that there is appropriate security for information we hold.

8. 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. Please contact the Security department if you have concerns regarding security measures taken to protect your information.

9. HOW LONG WILL WE KEEP THE PERSONAL DATA?

We currently retain your data permanently. However, we are in the process of identifying retention periods, creating a retention schedule, and applying controls to ensure data is weeded, anonymized or deleted as appropriate when it reaches its assigned period.

This does not affect your right to request data erasure. We will honor all such valid requests.

10. WHAT RIGHTS DO YOU HAVE?

To exercise any of the following rights, please contact hr@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.

We advise employees to discuss these matters with line management and HR before making a formal request, as we are completely transparent about the use of your data. We do have to make the distinction between data that is "about you" and data where you may be mentioned but you are not the focus of the information. For example, you may not have the right to be supplied with data that mentions you if it has the customer as its focus.

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.

11. 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 with HR.

You have the right to make a complaint at any time to the relevant local, national or industry privacy regulator.

12. WHAT IF YOU ARE A CALIFORNIA RESIDENT?

Congratulations, the California Consumer Privacy Act (CCPA) 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 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 the 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 employee data; data is collected directly from you.

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