

# Granicus, LLC Admins Privacy Statement (Last updated: May 18, 2018)

## 1. Overview

Granicus, LLC ("Granicus" or "We") 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, email address, and IP address are examples of personal data.

Unless otherwise specified, this statement applies to Granicus' Communications solutions, including Communications Cloud and Targeted Messaging Service.

Granicus 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.

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. 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.

- 1. Overview..... 1
- 2. Contact Us ..... 2
- 3. What Personal Data Does Granicus Collect, and for What Purpose?..... 2
  - Communications Suite..... 2
  - Customer Support ..... 3
- 4. Legal Basis for Collecting and Processing Data ..... 3
- 5. Change of Legal Basis..... 3
- 6. Failure to Provide Personal Data ..... 4
- 7. Profiling ..... 4
- 8. Do We Share Your Personal Data with Third Parties?..... 4
- 9. International Data Transfers ..... 4
  - Useful Privacy Shield Links ..... 5
- 10. Security..... 5
- 11. Data Retention..... 6
- 12. Data Subject Rights ..... 6
  - 12.1 Right to Request Access ..... 7
  - 12.2 Right to Rectification..... 7

12.3	Right to Object.....	7
12.4	Right to Erasure .....	7
12.5	Right to Restriction of Processing.....	7
12.6	Right to Portability .....	8
12.7	Right to Revoke Consent .....	8
12.8	Right to Make a Complaint.....	8

## 2. Contact Us

If you have any 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 [support@granicus.com](mailto:support@granicus.com). If you have additional questions or need to escalate an issue, use the below details for our Data Protection Officer (DPO).

Full name of legal entity: Granicus, LLC

Name or title of DPO: Gerry Hansen

Email address: [dpo@granicus.com](mailto:dpo@granicus.com)

Postal address: 408 St. Peter Street, Suite 600, St. Paul, MN 55102, USA

Telephone number: 01 651 925 5765

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. 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.

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

### Communications Suite

Through your interaction with our Communications suite, including Communications Cloud and the Targeted Messaging Service, we may collect the following information:

- Name, department, and title—used to identify the records you modified in the system.
- Your email address and phone number—to contact you regarding your activities in the Communications Cloud system and for two-factor authentication. This information is gathered either directly from you, or from our client (in many cases, your employer).
- Your answers to security questions, which may include personal data.
- A record of when you log in to the system—this is used to limit the number of unsuccessful login attempts during a given period of time. We also use these records, along with information regarding your browser user agent and IP address, for security, support, and auditing purposes.
- Your password, which is used to verify your identity.

## Customer Support

- When you contact our Customer Support department for assistance, we collect your name and email address so that we can communicate with you in the event your issue cannot be immediately resolved.
- We might proactively contact you via email to inform you of any technical issues with your account or the application in general.
- During this process, some identifiable information (IP address, browser user agent, and operating system) is collected for internal auditing and support purposes.

## 4. Legal Basis for Collecting and Processing Data

We will use your personal data when the law allows us to. Most commonly, as an administrator in the system, we will process your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you or your employer;
- 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.

Generally, we do not rely on your consent as grounds for processing your personal information other than in relation to sending marketing communications. Please see our [marketing privacy statement](#). Where we rely on your consent as a legal ground for processing, you have the right to withdraw consent at any time.

Our legitimate interests may include:

- Being efficient about how we fulfil our legal and contractual duties.
- Providing high quality customer service.
- Complying with laws or regulations that apply to us.
- Developing the Communications suite, our websites and other products and services, and what we charge for them.
- Contacting you with important information regarding the operation of our products.
- Developing and improving the network security, efficiency and technical specification of our IT systems and infrastructure.
- Providing our customers with the Communications suite, our websites, and other high-quality product and service features.

## 5. Change of Legal Basis

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. Failure to Provide Personal 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 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. Profiling

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?

Except as described here or in any of our other applicable privacy policies, we will not sell, distribute, lease, or provide any of your personal data to any third parties unless we have your permission to do so or are required by law.

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.
- **Third parties 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 to comply with a legal obligation, including 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 respond to an emergency, or as necessary for other legal purposes.
- **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.

## 9. International Data Transfers

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").

### Privacy Shield Certification

Granicus participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Granicus is committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List.

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.

With respect to personal data received or transferred pursuant to the Privacy Shield Framework, Granicus is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Granicus 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 has agreed to cooperate with the European Data Protection Authorities 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 Granicus 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, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

As a global company, Granicus employs a multifaceted approach to protecting personal data. For example, when transferring personal data 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 data needed and countries involved. Please contact Granicus for any questions you might have or for additional information regarding the protections in place to protect your personal data.

#### **Useful Privacy Shield Links**

- <https://www.privacyshield.gov/list>
- [http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm)
- <https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>

## **10. Security**

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 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.

## 11. Data Retention

How long we retain your data depends on the type of data and the purpose for which we process your data. Your data will not be retained for a period longer than necessary for the purpose for which we have processed your data, plus any statutory period during which we need to retain the data to resolve any legal claims. In many cases, this means that your data will be retained for the duration of our contract with our client, plus any legal statutory period. Information retained during the legal statutory period will be minimized to only the data strictly necessary to resolve any legal claims that may arise.

However, it may not always be possible to completely remove or delete all your personal data from our data bases 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.

## 12. Data Subject Rights

To exercise any of the following rights, please contact [support@granicus.com](mailto:support@granicus.com). If you need to escalate a matter or feel that your issue is unresolved, please contact our DPO.

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 if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

### **12.1 Right to Request Access**

You have the right to request details of your personal data that we hold. Upon request, we will provide a copy of such personal data within a reasonable timeframe.

### **12.2 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.

### **12.3 Right to Object**

You may choose to object to 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 on 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 our [marketing privacy statement](#).

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

### **12.4 Right to Erasure**

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

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

### **12.5 Right to Restriction of Processing**

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

- You contest the accuracy of the personal data.
- The processing of the data is unlawful.
- The personal data has reached the defined retention period, but you require the personal data to establish, exercise, or defend legal claims.
- 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 Granicus's legitimate grounds override your rights as a data subject.

### **12.6 Right to Portability**

You have the right to receive your personal data in a structured, commonly used, and machine-readable format. Granicus 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 information to perform a contract with you.

### **12.7 Right to Revoke Consent**

For certain data that you have specifically consented to be processed, you may revoke such consent at any time and request such information be deleted. An example of such data is your responses to security questions. However, if you withdraw your consent, this will not affect the lawfulness of any processing carried out before you withdraw your consent.

This right does not apply to information that is processed pursuant to our contract with your employer or information processed to protect the integrity of the controller's account. Examples of such data to which this right does not apply includes, but is not limited to, records of subscribers created, bulletins sent, and login attempts.

### **12.8 Right to Make a Complaint**

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.