Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The GovDelivery Communications Cloud (GovDelivery) is a web-based software system, provided by Granicus, that allows several FTC offices, including the Division of Consumer and Business Education, the Office of Public Affairs, and the Office of International Affairs, to deliver emails to subscribers and manage subscriptions. GovDelivery allows people to subscribe to a variety of email updates from the FTC including press releases, blog posts, and e-newsletters based on their individual needs and interests. The FTC also uses GovDelivery to distribute the FTC Daily(a)to sa   tton0002 Tc 0 11.0 Tw [and

their account settings, they can do so by clicking on the "Manage my email subscriptions" link at www.ftc.gov/stay-connected. They are prompted to enter their email address to subscribe or edit their current subscriptions, but a password is not required unless they have previously created one for their account.

The system maintains the user's email address, subscriptions, and password until they are changed or deleted by the user. Following standard security protocols, GovDelivery sign-up pages collect basic web log information, including IP address, pages accessed, pages requested, and time and date of access. The web log information is not linked to any individual accounts.

1.2

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check <u>all</u> that apply.

> PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

☐ Full Name
☐ Date of Birth
☐ Home Address
☐ Phone Number(s)
☐ Place of Birth
☐ Age
☐ Race/ethnicity
☐ Alias
☐ Sex
☒ Email Address
☐ Work Address
☐ Taxpayer ID
☐ Credit Card Number
☐ Facsimile Number
☐ Medical Information
☐ Education Records
☐ Social Security Number

	employees may access this data to provide FTC administrators customer support.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Granicus employees who are members of the support team will have access to the data in the system. All Granicus employees who will have access to the system are required to take Granicus' Security Awareness training and Insider Threat training. In addition, all employees are required to sign a non-disclosure agreement as well as sign the Acceptable Use Policy.

Granicus implements a rl Tc 0 Tw 2soI6 (r)-4o.6 (hsr)-1.9 acep,-t.9 so-1.9 (e r)-1o-1.9nlS 4ho ae

please read our privacy policy. We use GovDelivery, a contractor, to help us provide this service. According to our agreement, GovDelivery will not share your information with third parties. To learn more, read their privacy policy.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Subscribers must provide an email address in order to use GovDelivery's subscription services. Users who do not wish to provide this information would not be able to subscribe to GovDelivery's email services. Users may unsubscribe at any time by clicking on the "unsubscribe" link included in every email or by visiting a web-based subscriber preferences page where they can modify their email addresses, add, change, or delete a password, review their subscriptions, set delivery preferences, or delete their profile entirely.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Once users subscribe, they will have access to a web page where they can manage their email subscriptions. They can access the page by clicking on the "Manage Preferences" link in the footer of emails they receive from the FTC or by visiting the FTC subscriptions page at https://www.ftc.gov/stay-connected and clicking on "Manage Your Subscriptions." Once there, subscribers must enter the email address to manage their current subscriptions. Subscribers who have chosen to password-protect their web-based subscriber preferences page must enter the password to gain access to the page.

Subscribers are also provided with a customer service email address and phone number for any questions or problems they may have.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Subscribers must confirm their email address during the subscription process by entering it twice. Then they will receive a confirmation email that they have successfully subscribed. Users who fail to submit a valid email address will not be able to subscribe to GovDelivery services.

It is possible for a malicious actor to enter an email address and change or delete a subscriber's email preferences if the subscriber has not set a password on their account. In such cases, if the subscriber notices that they are receiving inaccurate subscription emails or no emails at all, the subscriber must access their own account and update or reactivate their preferred settings.

Granicus does not require users to set passwords on their accounts when they sign up for subscription services via GovDelivery. Due the minimal (and non-sensitive) personal information maintained in the system, Granicus has determined that requiring users to set passwords would be too burdensome on the customer. However, Granicus does give the user the option to set a password, if he/she so chooses. The user can use their email address to access

their subscription settings, and if they feel there has been erroneous activity on their account, the user can contact Granicus to report complaints, concerns, or any questions the user may have.

5 Data Accuracy and

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Granicus will retain a user's settings and subscription records for as long as the user subscribes to its services. When users unsubscribe, their preferences are immediately and permanently deleted. After one year, their email addresses are permanently deleted as well.

A full backup of the system is run on a daily basis and incremental backups are executed every five minutes. As such, any database activity (such as a profile deletion) is almost immediately incorporated in the backup structure.

The FTC will retain aggregate analytics data for only as long as is necessary for operational purposes. The data will be maintained in accordance with FTC regulations, policies, and procedures.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

The GovDelivery subscription pages use session cookies to allow subscribers to access and make changes to their profile. The session cookie stores the user's email address in order to identify the user and save changes. The cookie is not shared with other websites and expires as soon as the user closes the browser.

Granicus analytics track whether users open an email or click on links in an email. Clicks are measured by including unique, customized links in each email. When a subscriber accesses his or her unique link, then that is recorded as one click. Each email includes a unique, invisible image that is used to track whether users open an email. When a particular image is accessed, that is recorded as one "email open". The FTC can review this information in aggregate form through the GovDelivery Communications Cloud. No personal identifiers are associated or tagged with the email opened or the particular image associated with that email.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	Mitigation Strategy
Granicus could suffer a data breach	GovDelivery received FedRAMP certification in April 2016, hosts data in a secure center that includes five levels of physical security, and employs state-of-the-art firewalls.

terms of sensitivity, and the FTC collects only the information needed in order to send subscribers the messages they request.

9 Approval and Signature Page

Prepared By:

_____ **Date: _____**
Alvaro Puig
Chief of Staff
Division of Consumer and Business Education

Reviewed By:

_____ **Date: _____**
Katherine Race Brin
Chief Privacy Officer (CPO)

_____ **Date: _____**
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date: _____ 4ydohITJ 16.9TJ ( )T**