

GRS Mobile and Web Application Privacy Notice

Date of last revision: November 7, 2022

Welcome to Global Response Systems' ("GRS") mobile and web application ("GRS App" or "Service"). The GRS App is operated by Global Response Systems, Corp. ("Global Response Systems", "GRS", "Company", "we", "our", or "us").

GRS is committed to protecting the privacy and security of your personally identifiable information. This Privacy Notice explains how we collect, use, share, protect and disclose your Personal Information, Usage Data and Message Data (as those terms are defined below) when you use the GRS App, website (the "Site") or GRS' cloud-based software-as-a-service (SaaS) enterprise messaging solution (collectively with the Site, the "Services"). This policy describes the choices that a User and a Customer (defined below) have regarding the collection and use of personal information from or through the GRS App. It applies only to information collected, used or stored through the GRS App; it does not apply to any other information collected or obtained through other means or to information collected by third parties. By using the Services you consent to this Privacy Policy.

BACKGROUND

This Privacy Notice establishes terms and conditions that apply to "Customers" and "Users". "Customers" are businesses and other entities that have separately executed a contract with GRS for the provision of a suite of software applications and other services ("Services Agreement").

In the course of the day-to-day operations of these Customers, and in connection with the performance of the Services Agreements, these Customers may require their employees (and contractors or other third parties, as applicable) ("Employee") to use the GRS App on smart phones, tablets, laptops, and/or desktops ("Device(s)"). Each such Employee may own the Device or may have received it from the Customer for use in the context of their employment with the Customer. The conditions for the use of these Devices in connection with a Customer's business or operation – for example when or how a Customer may monitor the use of a Device - are solely determined by the Customer and the Customer is solely responsible for communicating these conditional requirements to the Employee. GRS has no information and disclaims any liability for the manner in which an Employee uses a Device for any purpose.

In order to use the GRS App, an Employee must use a user ID and password provided by the Customer. The GRS App cannot be used, and cannot collect any data or information unless the Employee uses that user ID and password.

The Customer's GRS Administrator(s) may also enforce a password policy for devices running the GRS App. In order to support this functionality GRS Applications may require that you accept that password policy in order to use the GRS App.

An individual who has downloaded the GRS App on a Device and has been able access the GRS App as explained above is deemed a "User".

IMPORTANT: Users should not have any expectation of privacy when using the GRS App on any Device.

When you register for the GRS App, we collect information that personally identifies you, such as your name, address, mobile telephone number, e-mail addresses and other information that you provide to us ("Personal Information"). You may be asked to provide us and/or the

Customer with certain Personal Information when you register to use the Services, and at other times. The decision to provide this information is voluntary. However, if you choose not to provide the requested information, you may not be able to use certain features of the Services. Unless otherwise provided in a separate agreement, all uses of the GRS App are deemed made by Users on behalf of, and for the benefit of, the GRS Customer who provided that User with the agreed upon user ID and initial password. The GRS Customer is the only entity authorized to make decisions regarding the personal information collected by the GRS App, including, without limitation, decisions about deletion or disposal of information.

This Privacy Notice describes how GRS handles the personal information of the Users of the GRS App that is collected or processed by a Device on which the GRS App is installed.

To the extent that the GRS App is used to collect or transmit information about other individuals, for example clients or patients of a Customer, the policies regarding the handling of this other information are provided in a separate document.

CONSENT AND MODIFICATIONS

The use of the GRS App by a User signifies the User's agreement to the terms of this Privacy Notice. Customers and Users should ensure that they read this Privacy Notice carefully.

GRS may modify this Privacy Notice from time to time and will notify Users and Customers of material changes to this Privacy Notice by posting the amended terms in accordance with applicable laws. Any User who does not agree with the proposed changes should notify the Customer and cease using the GRS App before the new Privacy Notice takes effect. Should a User continue using the GRS App after the new terms take effect, that User will be bound by the modified Privacy Notice.

Any User who does not agree with GRS' current or updated Privacy Notice(s), may at their discretion, elect to uninstall the GRS App using methods provided by their Device's manufacturer. Please see also the section "Removal or Disposal of Information"

INFORMATION COLLECTED BY GRS

GRS, and in some instances its Customers, collect information from users when they interact with the GRS App.

Registration Information: Information the User provides when first accessing the GRS App, for example, the User's phone number and work email address.

Electronic Communications: Electronic communications the user chooses to share with GRS, such as support requests.

Device Information: The type of Device on which the GRS App is downloaded, operating system name and version, device manufacturer, application version, device ID, IP address, SSID, and connection strength.

Log file information: Log files that record each time a Device accesses secure servers, and information about the Device.

Usage Information: Information about how the user uses the GRS App, such as time, response types, User name and manner of use and interaction with the GRS App; date stamp, type of access.

Photos: If granted access to the device, the GRS App has access to all photos taken within the GRS App, and allows Users to select and upload the selected photos to the GRS App for transmittal to the Customer.

Messages: Text messages that are sent within the GRS App.

Metadata: When a User uploads photos, the GRS App stores the metadata associated with the photo, such as time and location information, associated with that specific photo.

USE OF INFORMATION

In addition to some of the specific uses of information that are described in this Privacy Notice, we may use information we collect to:

- Facilitate the use of the Service;
- Send users electronic communications about the Service or to respond to inquiries, or requests for support;
- Archive the content of each user's account;
- Improve, test, and monitor the effectiveness of the GRS App;
- Compile statistics regarding the use of the GRS App, to identify usage trends;
- Develop features on the GRS App that may be of interest to users;
- Perform data analysis, audit, fraud monitoring and prevention;
- Perform any other functions that we believe in good faith are necessary to protect the security or proper functioning of the GRS App

SHARING OF INFORMATION

Except as noted in this Privacy Notice, GRS does not disclose a User's information to third parties without giving the User and the Customer prior notice.

- **Customer**

Unless otherwise agreed between Customer and GRS, all data or information transmitted, collected or stored by the GRS App belongs to the Customer. Thus, we may, upon a Customer's request, provide the Customer access to all data or information created, received, sent, stored or other processes by the GRS App on a User's Device.

- **Third-Party Services**

We may provide users' information to third parties that we retain for operating, maintaining, repairing, or otherwise improving or preserving the Service.

- **Responding to legal requests and preventing harm**

We may disclose information about, or associated to a User or User account to a third-party in response to a facially valid request from a government agency or a private litigant in the form of a subpoena, court order or search warrant, or where we believe, in good faith, that it is necessary to do so for the purposes of a civil action, criminal investigation, other legal matter.

- **Change of Control**

GRS has established business relationships with other businesses that we believe are trustworthy and who have demonstrated privacy practices that are consistent with ours (“Service Providers”, “Business Associates”). For example, we may contract with Service Providers to provide certain services, such as hosting, maintenance, security and audits. We provide our Service Providers with only the information necessary for them to perform these services. Each Service Provider must agree to use reasonable security procedures and practices, appropriate to the nature of the information involved, in order to protect your Personal Information and Message Data from unauthorized access, use or disclosure. Service Providers are prohibited from using Personal Information or Message Data in any manner other than as specified by us.

- **Change of Control**

We may disclose information about our Customers to a third-party in the event of reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any of our business, assets, or stock, including in connection with bankruptcy or similar proceedings.

- **Compliance with Laws and Law Enforcement**

GRS cooperates with government and law enforcement officials to enforce and comply with the law. We may, therefore, disclose Personal Information, Usage Data, Message Data, and any other information about you, if we deem that it is reasonably necessary to: (a) satisfy any applicable law, regulation, legal process (such as a subpoena or court order) or enforceable governmental request; (b) enforce the Terms or the Services, including investigating potential violations thereof; (c) detect, prevent, or otherwise address fraud, security or technical issues; or (d) protect against harm to the rights, property or safety of GRS, its users or the public as required or permitted by law.

DATA RETENTION AND STORAGE

GRS or one of its Service Providers will retain data and information collected or generated by a User through the use of the GRS App in accordance with the direction GRS receives from the Customer, as necessary to comply with our legal obligations, resolve disputes and enforce our agreements. If we do not receive any written instruction from the Customer, we will retain all data or information in accordance with our data retention policy.

All data and information is stored in the United States. By using the Services, you agree that the collection, use, transfer, and disclosure of your information and communications will be governed by the applicable laws in the United States.

ACCOUNT DEACTIVATION

Customers have the ability to deactivate, suspend or terminate a User’s GRS account. For assistance, Customers should contact us as set forth in the “How to Contact Us” section, and we will provide any required assistance.

Any User who wishes to deactivate or terminate his/her account, or remove specific data in his/her account should first contact the Customer. We will follow written instructions sent by or on behalf of the Customer unless they conflict with the section “Data Retention.”

DISPOSAL, OR ERASURE OF INFORMATION

Any User may at any time delete or remove the GRS App from the User's Device by following the Device Manufacturer's instructions.

When a User uses the GRS App on the User's Device, a copy of all information collected, generated, or stored by the GRS App on that Device may in certain circumstances be stored on GRS Service Provider's servers. When the GRS App is removed from a User's Device, all information previously collected, generated or stored by the GRS App, while no longer accessible from the Device, remains stored on the Service Provider's servers.

Unless GRS is required by applicable law or court order to take a specific action (e.g. preservation, duplication, storage, disposal) with respect to such data or information stored by its application on GRS' Service Provider servers, GRS will follow the Customer's written instructions with respect to the preservation or disposal of such data or information, or if there are not such instructions, will retain such information in accordance with its applicable data retention policy.

INFORMATION SECURITY

We take reasonable measures to protect any personal information we may hold in order to prevent loss, misuse, unauthorized access, disclosure, alteration and destruction.

Users should not disclose any user ID or password required to access the GRS App to any third party unless otherwise instructed by Customer and communicated in writing to GRS. Each User and Customer will be responsible for any use of GRS under that User's user ID and password unless they have notified GRS (in addition to notifying Customer) in writing of the loss or compromise of such information in accordance to the "How to Contact Us" section, and GRS has acknowledged receipt of the notice.

Regardless of efforts, no data transmission over the Internet or other network, including any of GRS' services, can be guaranteed to be 100% secure. Accordingly, we cannot and do not guarantee the absolute security of any information you transmit on or through the Services and any information you transmit is sent at your own risk.

PRIVACY RIGHTS

GRS does not share any personal information about a User with outside third-parties for their direct marketing purposes.

HOW TO CONTACT US

If you have any questions about this Privacy Notice, please contact us by email at info@securegrs.com