PRIVACY POLICY

Last modified: January 9, 2018

Thank you for using our Global Data Sciences, Inc. ("GDS" and/or "EIE", "We", "Our") Website, Apps and/or Services. EIE allows you to encrypt and send audio, video, photos, voice, documents, text messages, and other formats so that you can easily communicate safely and securely.

This document, our Privacy Policy ("Privacy Policy"), governs how EIE ("We," "Us," etc.) handles our users ("You," "Your," etc.) data both in the EIE Apps themselves (the "EIE Apps") and on our website/servers (collectively, the "Services").

Our Privacy Policy is incorporated into and is subject to the EIE Terms of Service, so please read both documents carefully. Your use of the EIE Services indicates your consent to this Privacy Policy and our Terms of Service. If you do not want to be bound by these Agreements, you may not use our Services.

We work very hard to preserve your privacy and security, and we do our best to be as transparent as possible in explaining how we use your data in providing our Services. Please contact us if you have any questions at info@encryptedinfoex.com.

Our Privacy Practices, in Brief:
EIE has to collect some information from you in order to provide our Services to you, but we do so in a highly limited, highly secure way.

- We can't see information you give us. Your information is always disguised with multiple layers of encryption before it is transmitted to our servers. Because of this we don't know — and therefore can't reveal to others — anything about you or how you use the EIE App aside from the date your account was created and the date of last use.
- EIE deletes all metadata from your messages and media.
- Deletion is forever. When you delete a message, or when a message expires, we use forensic deletion techniques to ensure that your data can never be recovered by us or anyone else.

- Depending on your device, screenshots may or may not be possible. On iOS and desktop, screenshots are possible – due to a requirement imposed by Apple. Please note that, if someone you communicate with on EIE App takes a screenshot of your conversation on his or her iOS device, we will immediately notify you via a message and indicate what was captured in that screenshot. There are no screenshot notifications available on EIE desktop.
- We cannot prevent someone using a camera to take a picture of a message on a screen. Therefore, we strongly encourage you to only send private messages or sensitive information to people you know and trust.
- You own your data. We do not share or sell any data about our users.

What Information Does EIE Collect and How Is It Used?

We are committed to limiting our collection of your information to what is necessary to provide you with our Services.

We only collect information from users who create EIE Accounts. You must create a EIE Account to use the EIE App.

- Information We Collect:
    - Personal Information – When you create an account, you will be required to provide us with personal information about yourself, which may include your name, e-mail address, and phone number (collectively, "Personal Information"). We do not collect any Personal Information from you when you use the EIE Services unless you voluntarily provide us with the Personal Information. The Personal Information is used to provide the requested Service, and occasionally to contact users of our Service to notify them of our current and future products and offerings.
    - Message Information – When you use the EIE Service to send and/or receive encrypted Messages, we may temporarily process and store your message (in encrypted form only), log and contact data, and other related information (collectively, the "Message Information") in order to provide the EIE Services to you. We do not read your encrypted messages, and we forensically delete your messages at the appropriate time and on the appropriate devices.
    - Billing Information – If users wish to purchase a Subscription for any premium features we may offer in the future, they may be required to provide certain information in addition to the information noted above. Such information may include a debit card number, credit card number, expiration date, bank account information, billing address, activation codes, and similar information. Such information is collectively called the "Billing Data." Such Billing

Data would be collected and processed by a third-party payment vendor pursuant to the terms and conditions of its privacy policy, and we would not obtain access to any Billing Data in connection with these transactions.

What We Don't Collect: Important to us is the information we don't collect. We do not collect any location information or have access to the contents of the communications you send using the EIE App. After messages are deleted (or after they expire), they are forensically deleted and are not retrievable by us or anyone else. (Remember, however, that if you send a EIE message to another EIE user, that message might remain on their device even after you delete it from yours, depending on whether the recipient took a screenshot of the message.)

- Information We Use But Do Not Collect:
    - Address Book Information – When you access and use the EIE Services, you may grant us the right to access and use the information within your Address Book. This information will only be used within the EIE Services at the time of action and will never be stored or used in any other manner by the EIE Services
    - Geo-location Information – Certain features and functionality of the EIE Services may be based on your location. In order to provide these features and functionalities we use – based on your consent – geological information from your mobile device or wireless carrier and/or certain third party service providers. Such information is used only to either (a) set a geo fence rule, or (b) validate a geo fence rule. After rule validation, the geo information is removed and deleted.

User-Provided Information: We collect some very limited information from you after you download the EIE Apps in order to allow you to create a EIE Account, and begin using the EIE App.

- **Your EIE ID:** Your EIE ID is how you allow others to contact you via EIE. It does not have to be your real name or provide any reference to your identity. Like other information pertaining to your account, it is disguised with multiple rounds of encryption. The purpose of this encrypted representation is to allow you to use our Services without our needing to know who you are.
- **Your Password:** We require you to have a password to use the EIE App, but we never store your password in an unencrypted format. For your own security, we recommend that you use a long, unique password consisting of a mix of upper and lower-case letters, numbers, and symbols.

Optional User-Provided Information: Within the EIE App, we provide a few optional features for your convenience. Some of these features, described below, will ask for personal information. If you want to keep

your use of EIE as anonymous as possible, please read these sections carefully in order to understand how we associate information you provide with your EIE Account.

- **Push Notifications:** When setting up your EIE Account, we will ask if you want to receive notifications of new EIE messages, software updates, and other administrative and technological developments. Push notifications are functions of devices operating system, so if you enable this feature, your devices operating system's manufacturer will know that you are using the EIE App, but will not know anything about how you use it or be able to see anything you transmit through it.
- **INVITE:** If you use the feature to send EIE Invitations, the EIE App will be able to access your device's contacts in order to invite them to use our Services. We never store your device contacts on our servers in any way. All invitations are generated locally on your device, without sharing any information with us.
- **Remember Me Login:** By default, the EIE App will require you to provide your username and password in order to use the EIE App. If you use the Remember Me function, the EIE App will automatically have your username and password filled in for you. While you will still benefit from EIE's security (e.g., deletion, encryption, etc.) and may find that your user experience is more seamless, this option is less secure than the default logout and password requirements, and we suggest that users who enable Remember Me retain other security measures on their devices, like enabling screen locks, PINs and fingerprint security through your device settings. You can also use the fingerprint security through your device settings, if you device supports this feature.

Automatically Collected Information: EIE collects a small amount of information automatically during your setup and use of the EIE App: Aggregate Usage Data.

- **Aggregate Usage Data:** During the operation of our services, we also collect aggregate, anonymous information about basic usage statistics, such as the number of messages sent by all EIE users daily, what types of messages our users tend to send (e.g., voice messages more often than text), and so forth. We never attempt to (and cannot) identify users associated with any of this information.

What Information Does EIE Share with Third Parties?

Like many businesses, we hire other companies to perform certain business-related services. We may disclose personal information to certain types of third party companies but only to the extent needed to enable them to provide such services. The types of companies that may receive personal information and their functions are: marketing assistance, data storage, hosting services, customer support, and payment processors. All such third parties function as our agents, performing services at our instruction and on our behalf pursuant to contracts which require they provide at least the same level of privacy protection as is required by this privacy policy and implemented by EIE. You may opt out of having your personal information transferred to any or all of our categories of agents by contacting us at info@encryptedinfoex.com. Please allow us a reasonable time to process your request. If you opt out of having your personal information transferred to certain categories of agents, you may not be able to use certain functionality of our Website and the Service.

We do not currently collect sensitive personal information from you. If we start collecting your sensitive personal information in the future, we will not disclose your sensitive personal information to any third party without first obtaining your opt-in consent. If/when applicable, you will be able to grant such consent by contacting us at info@encryptedinfoex.com.

In each instance, please allow us a reasonable time to process your response.

Business Transfers

In the event of a merger, dissolution or similar corporate event, or the sale of all or substantially all of our assets, we expect that the information that we have collected, including personal information, would be transferred to the surviving entity in a merger or the acquiring entity. All such transfers shall be subject to our commitments with respect to the privacy and confidentiality of such personal information as set forth in this Privacy Policy.

Disclosure to Public Authorities

We will always notify you of any third party requests for your information unless legally unable to do so. As soon as legally permitted to do so, we will notify our users of requests for their information. We require a warrant before handing over the contents of your communication, however, because of the nature of our technology, the contents of your communication will be undecipherable if obtained.

You Can Deactivate Your Account

You can deactivate your account at any time. Once deactivated your account will be irrevocably suspended, ensuring that nobody can use that EIE ID again in order to prevent impersonation. If you wish to deactivate your EIE account, go to EIE Settings, Account, tap “Delete Account” and verify by entering your password.

We Retain As Little Data As Possible, for the Least Time Possible

Data Retention on EIE’s Servers: Our servers store the encrypted messages that you send and receive until either you: (a) delete the message, or; (b) the message is auto-deleted by virtue of rules established for that message. We retain non- message data (i.e. Types of messages) for as long as you use the EIE Services and for an indefinite time thereafter.

Data Retention on Your Device: All messages are presented in encrypted form on end users’ devices, and are available in a viewable format only after you open the communication. Your messages are never retained on

your device, and the device's memory is cleared upon either; (a) logging out of the App; (b) closing the message, or; (c) deleting the message. Deleted messages can never be recovered.

We Are Serious About Security

We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees who need to know that information in order to operate, develop, or improve our Services. No sensitive information is in the clear: we take reasonable efforts (as described herein) to ensure that everything we store is not retrievable by us or anyone else.

However, as security experts, we know that no security system can prevent all potential security breaches. Therefore, we have limited the potential implications of such a breach by designing our system so that in the event of a breach, we would have the least possible information about you.

Children and COPPA

We do not maintain any personally identifiable information about our users or their communications. You can learn more about the information EIE does and doesn't collect here.

EIE is not directed to children under the age of 13. If we learn that we have collected personally identifiable information from a child under 13, we will take appropriate steps to delete such information as soon as possible. If you are under 13, please do not use the EIE Services or give us any Personal Information. We encourage parents and legal guardians to monitor their children's Internet usage and to help enforce our Privacy Policy by instruction their children to never provide us Personal Information without their permission. If you have reason to believe that a child under the age of 13 has provided Personal Information to us, please contact us, and we will use commercially reasonable efforts to delete the information from our databases, though there can be no assurance that we are able to do so.

Customer Service

Any information provided to us by our users voluntarily when they request customer support (e.g., an email address) will be used to respond to that individual request and may be logged as part of our effort to improve our customer service and solve any product-related issues. These email addresses cannot be linked to our users' EIE accounts, unless users voluntarily include their EIE account information in their customer service-related requests. We strongly discourage our users from disclosing their login and password information. We will never request your login and password.

Users Outside the US

If you use our Services and reside outside the U.S., your information will be transferred to the U.S. and will be processed and stored there under U.S. privacy standards. By using our Services and providing information to us, you consent to such transfer to and processing in the U.S. Except in the case of data transfers under the EU-US Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework, your decision to provide such data to us, or allow us to collect such data through our Website, the App or the Service, constitutes your consent to this data transfer.

EIE complies with the EU-US Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from the European Union member countries (including Iceland, Liechtenstein and Norway) and Switzerland to the United States, respectively. EIE has certified that it adheres to the Privacy Shield principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, Recourse, Enforcement and Liability (the "Privacy Shield Principles"). If there is a conflict between this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.

You are responsible for complying with any laws or regulations in your country that govern use of Apps and Services like EIE.

California Privacy Rights

Pursuant to Section 1798.83 of the California Civil Code, residents of California have the right to obtain certain information about the types of personal information that companies with whom they have an established business (and that are not otherwise exempt) have shared with third parties for direct marketing purposes during the preceding calendar year, including the names and addresses of those third parties, and examples of the types of services or products marketed by those third parties. If you wish to submit a request pursuant to Section 1798.83, please contact EIE at info@encryptedinfoex.com. In addition, EIE does not monitor, recognize, or honor any opt-out or do not track mechanisms, including general web browser "Do Not Track" settings and/or signals.

External Websites

The Website, the App and the Service may contain links to third-party websites. EIE has no control over the privacy practices or the content of any of these websites. As such, we are not responsible for their content or privacy policies. You should check the applicable third-party privacy policy and terms of use when visiting any other websites, and before providing any personal information to such external sites.

We Can Change This Privacy Policy

This Privacy Policy may be updated from time to time, for any reason. We will notify you of any changes to our Privacy Policy by posting the new Privacy Policy here. You are advised to consult this Privacy Policy regularly for any changes.

Contact Us if You Have Questions

If you have any questions regarding privacy while using our Services, or have questions about our practices, please contact us via email at info@encryptedinfoex.com.