Privacy Policy

(Revised on October 10, 2018)

Szeto Technologies manufactures and supplies equipment to the Service Providers (example: your telephone answering service). The privacy policy described here is purely based on the technical and architectural design of the equipment. Whatever information collected from the users is solely for the purposes of operation. This information is stored in the equipment and is maintained by your Telephone Answering Service provider.

Szeto Technologies takes extreme measures and careful considerations in designing its equipment to protect the privacy and security of your personal information. This Privacy Policy explains how we collect, use, protect, and disclose your Personal Data, Usage Data and Message Data (as those terms are defined below) when you use our mobile app, “SMessages”, “Work-Alone”, or visit the Szeto Technologies “Web-Site”, (hereon collectively referred to as “Services”).

1. INFORMATION WE COLLECT

Personal Data

When you register for “SMessages” mobile app, you enter information that personally identifies you, such as your name (Full Name), identification (SCMid), password (Password), mobile telephone (Cellular Number) and other voluntary information that you might have entered in (Description). Optionally, you might enter your contact lists (Group Name) containing the team members which allow the mobile app to connect users of the Service and place them in the appropriate user groups (you might withdraw or modify this information at any time). As such, we may indicate who in your connections are also users of the Service, and likewise we may indicate to your connections the same regarding you. This feature allows you to connect with other users of the Service and may allow other users of the Service to communicate directly with each other. If any of the group information is modified by you or other members, the data will be updated instantly. The software does not keep records of the previous settings. Please note that the members are limited to a “closed” group of people, such that all team members are subscribers of the same “SMessages” service, usually are the employees of the same organization.

When you register for the “Work-Alone” mobile app, your personal information, such as your name (Full Name), employee identification # (PEid), password (Password), mobile telephone (Cellular Number), monitoring service’s web address (URL) and other voluntary information that you might have entered in the (Description), together with the automatic current (GPS) location, will be stored in a record to allow us to trace your physical locations in the case of emergency. These data are kept in a file for later reviews and reports. The maximum storage time
of this information is 3 months, or when the employee is no longer with the company, or when the monitoring service is terminated, whichever comes first.

When you access a web-site (namely the Szeto “Call Linx” Web-Page) to view personal messages, programming on-call, making appointments, etc., your Telephone Answering Service provider will assign you a log-in (User Name) and (Password). This information is used to authenticate your access to the web-page and retained in the database until your access is no longer required. They can be changed at anytime if deemed necessary. The changed information will overwrite the old data in the database.

Usage Data

We automatically keep track of the usage information that allows us to generate the billing information and statistical reports to our service provider clients, regarding how users access and use the Services (Usage Data). For example, when you download and use Service “SMessages” or “Work-Alone”, we automatically collect information on the type of device (Android / iPhone / Blackberry) that you use, the model of the phone, the device operating system, etc. This information is temporary stored in a memory log file to optimize the software for power consumption of the particular type of device, and also to be used as a reference for debugging in case of any users reporting an issue about the mobile app with their phones. However, in the “WorkAlone” application, the type of device (iPhone, Android, Blackberry) may also be programmed by our clients (the answering service providers) via the WorkAlone portal and they are therefore be available to those other employees of the same company who are programmed with the access to the WorkAlone web pages by our clients.

When you access our “Call Linx” Web Page, we do not collect information regarding the following: type of web browser you use, your operating system, your Internet Service Provider, the pages you view on our Site, the time and duration of your visits to the Site, or any information relating to your use of the Services. Your IP address used in accessing the web-page is only kept until you log off. It is not stored in the database.

Message Data

When you send or receive messages using our “SMessages” Service, we store your messages (“Message Data”) to provide these Services to you. After its delivery, Message Data is normally retained in the system database for a maximum period of 1 year. These messages can also be archived onto a separate storage medium as redundancy back up in case of equipment hardware failure. It is up to your Answering Service provider to determine the maximum time of keeping these backup media.
“Cookies” & “Do Not Track”

Like many other websites, we use cookies on the Site (a small removable data file that is stored by the web browser on your computer that identifies your computer and browser when you visit our Site or use our Services). We do not use cookies to collect Personal Information but rather to improve the quality of the Services. Most web browsers are initially set up to accept cookies. You can reset your web browser to refuse all cookies or to indicate when a cookie is being sent. Please note, however, that certain features of the Site may not function if you delete or disable cookies.

*The site’s cookies do not and cannot infiltrate a User’s hard drive to collect any information stored on the hard drive.*

Additionally, we do not track any of your online activities over our “Call Linx” website.

2. HOW WE USE THE INFORMATION WE COLLECT

Any information we collect from your using of our mobile apps and/or web-page is for internal system function purposes only. We do not sell or rent information about you. We will not disclose information to third parties without your consent, except as explained in this Privacy Policy.

3. HOW WE PROTECT THE INFORMATION WE COLLECT

Security

Szeto Technologies, Inc. is committed to protecting the security of your information. We employ what we believe are industry best security measures designed to protect your information from unauthorized access. Regardless of efforts, no data transmission over the Internet or other network, including any of Szeto Technologies’ 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 are sent at your own risk.

We should also point out that the equipment that offers your service is purchased and owned by your service provider (the Answering Service), this information is stored in the equipment located in their premises. Although it is the best intention and the utmost effort of both parties to protect the security of collected information, we cannot control and be responsible for the procedures in what the other party adopts in safeguarding the said information.
Compliance with Laws & Law Enforcement

Szeto Technologies and its customers (the answering services) cooperate 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 Szeto Technologies, its users or the public as required or permitted by law.

4. CHANGES TO THE PRIVACY POLICY

We may periodically change this Privacy Policy. If we decide to change this Privacy Policy, we will inform you by posting the revised Privacy Policy on the Site. Those changes become effective upon posting on the Site, the date of which is shown as the “Revised On” date in the revised Privacy Policy. Use of information we collect now is subject to the Privacy Policy in effect at the time such information is collected. By continuing to use the Services, you agree to be bound by the revised Privacy Policy.

[End of Privacy Policy]