

## Lighthouse Privacy Policy

Groupe GSOFTE Inc. (“**GSOFTE**”) offers the security and compliance tool and platform commercialized by GSOFTE as “Lighthouse” that tracks Slack Users’ activities in Slack and that sends alerts in respect of such activities (“**Lighthouse**”). GSOFTE understands the importance of protecting personal information. For this reason, GSOFTE strives to have business procedures and security safeguards in place to protect personal information under its control.

### Application and Scope

This Privacy Policy (“**Policy**”) is intended to establish responsible and transparent practices for the management of personal information and to satisfy the relevant and applicable legal requirements. This Policy sets out the standards, responsibilities and obligations of GSOFTE in respect of any personal information collected, accessed or processed by GSOFTE when customers have access to and use Lighthouse and specifies the obligations of GSOFTE that arise from Lighthouse Terms of Service (available at <https://www.lighthousebot.com>) (the “**Terms**”) entered into between GSOFTE and its corporate customers (each, a “**Customer**”), whereby GSOFTE might handle or have access to personal information.

### International Compliance

GSOFTE complies with: (i) data protection laws applicable to GSOFTE; and (ii) applicable industry standards concerning data protection, confidentiality or information security. GSOFTE has global operations and therefore, in some cases, information managed by GSOFTE may be transferred, processed and stored to other countries, although at all times, GSOFTE will ensure that personal information is protected by confidentiality and security procedures and protections that are, at a minimum, equivalent to those employed by GSOFTE itself.

GSOFTE complies with this Policy as well as applicable Canadian private sector data protection laws such as the *Personal Information Protection and Electronic Documents Act* (“**PIPEDA**”) and substantially similar provincial laws pertaining to the collection, use and disclosure of personal information. PIPEDA provides for an adequate protection of personal information according to the European Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and the Council.

### Definition of Personal Information

Personal information is defined as “any information about an identifiable individual”. This may include, for example, email addresses and contact details and any similar information provided to GSOFTE when customers have access to and use Lighthouse, or which GSOFTE may receive from business inquiries about Lighthouse. Personal information that is aggregated and cannot be associated with an identifiable individual is not considered to be personal information.

## Collection and Use of Personal Information through the Services

When providing services, GSOFT only processes personal information in accordance with the Terms and applicable laws. GSOFT generally uses personal information from or about its Customers (hereinafter referred to as “**Customer’s Personal Information**”) for the following purposes:

- to create, establish and administer Customer’s account, to respond to Customer’s inquiries related to its account and to contact Customer about Lighthouse or account-related matters;
- to provide Customer with access to and use of Lighthouse and customer support;
- to measure and analyze Customer behavior in order to, among others, monitor, maintain and improve Lighthouse and to create new services or features;
- to meet legal and regulatory requirements and to allow GSOFT to meet contractual requirements relating to Lighthouse;
- to conduct surveys on the quality of Lighthouse or to collect feedbacks on Lighthouse; and
- to provide Customer with offers for additional products and services that GSOFT believes may be of interest to Customer.

GSOFT may also use information provided by Customers to create de-identified data aggregated for benchmarking or marketing purposes.

Unless required or authorized by law, GSOFT will not use Customer’s Personal Information for any other or new purpose without obtaining prior consent.

## Sharing of Personal Information

GSOFT will not sell, rent or trade personal information to any third party. However, GSOFT may share personal information when authorized and/or required by law or as follows:

- **Service providers.** GSOFT may grant access to personal information to third party service providers in connection with the performance or the improvement of Lighthouse. Before sharing any personal information with any of its third party service providers, GSOFT will ensure that the third party maintains reasonable data management practices for maintaining the confidentiality and security of personal information and preventing unauthorized access.
- **As permitted or required by law.** GSOFT may disclose personal information as required by applicable law or by proper legal or governmental authority. GSOFT may also disclose information to its accountants, auditors, agents and lawyers in connection with the enforcement or protection of its legal rights. GSOFT may also release certain personal information when it has reasonable grounds to believe that such release is reasonably necessary to protect the rights, property and safety of others and itself, in accordance

with or as authorized by law. In the event GSOF receives a governmental or other regulatory request for any Customer's Personal Information, it agrees to immediately notify Customer in order that Customer shall have the option to defend such action. GSOF shall reasonably cooperate with Customer in such defense.

- **Business transaction.** GSOF may disclose personal information to a third party in connection with a sale or transfer of business or assets, an amalgamation, re-organization or financing of parts of our business. However, in the event the transaction is completed, personal information will remain protected by applicable data protection laws. In the event the transaction is not completed, GSOF will require the other party not to use or disclose the personal information received in any manner whatsoever and to delete such information.

### **Security of Personal Information**

GSOF will store and process the personal information in a manner consistent with industry security standards. GSOF has implemented technical, organizational and administrative systems, policies, and procedures to help ensure the security, integrity and confidentiality of personal information and to mitigate the risk of unauthorized access to or use of personal information, including (i) appropriate administrative, technical and physical safeguards and other security measures designed to ensure the security and confidentiality of the personal information it manages; (ii) a security design intended to prevent any compromise of its own information systems, computer networks or data files by unauthorized users, viruses or malicious computer programs; (iii) appropriate internal practices including, but not limited to, encryption of data in transit; using appropriate firewall and antivirus software; maintaining these countermeasures, operating systems and other applications with up-to-date virus definitions and security patches so as to avoid any adverse impact to the personal information that it manages; appropriate logging and alerts to monitor access controls and to assure data integrity and confidentiality; permitting only authorized users access to systems and applications; and (iv) all persons with authorized access to personal information must have a genuine business need-to-know prior to access ("**Security Program**").

### **Training and Supervision**

GSOF maintains adequate training programs to ensure that its employees and any others acting on its behalf are aware of and adhere to its Security Program. GSOF shall exercise necessary and appropriate supervision over its relevant employees to maintain appropriate confidentiality and security of the personal information it manages.

### **Data Incidents involving Customer's Personal Information**

GSOF shall immediately notify Customer of any reasonably suspected or actual loss of data or breach or compromise of its Security Program which has or may result in the loss or unauthorized access, disclosure, use or acquisition of Customer's Personal Information (including hard copy records) or otherwise presents a potential threat to such information ("**Data Incident**"). While the initial notice may be in summary form, a comprehensive written notice shall be given within 48 hours to Customer. The notice shall summarize in reasonable detail the nature and scope of the Data Incident (including each data element type) and the corrective action already taken or to be

taken by GSOF. GSOF shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with Customer in all reasonable efforts to mitigate the adverse effects of Data Incident and to prevent its recurrence.

### **How to Contact Us**

Any questions or complaints regarding this Policy or GSOF handling of personal information when customers have access to and use Lighthouse can be addressed by sending an email to [admin@lighthousebot.com](mailto:admin@lighthousebot.com).

### **Change of Privacy Policy**

GSOF will review and update its policies and procedures as required to keep current with rules and regulations, new technologies, standards and customer concerns. This Policy may therefore change from time to time.

This Policy was last updated on November 28th, 2017.