Service Data Privacy Statement

Last updated in May 2018.

This Privacy Statement is intended to supplement and clarify the Sherweb Privacy Policy with regard to Personal Data processed on behalf of our Customers during provision of the Services. This Service Data Privacy Statement (“Privacy Statement”) is incorporated by reference in your Master Service Agreement (“MSA”). Your use of Services under the MSA is subject to the Privacy Statement. Unless otherwise defined in the Privacy Statement, capitalized terms have the meaning given in the MSA.

Definitions
Scope of this Privacy Statement
Data we Process
Purposes of Processing
How we Protect Data
Transparency and Cooperation with Customers
Sharing and Disclosures
Location of Service Data
Data Retention
Data Subject Rights
Changes to this Statement
How to Contact Sherweb

1. Definitions

“Customer” means a legal entity with whom Sherweb has an agreement to provide the Services. For clarity, a Customer may be a Controller or a Processor of Personal Data. Where a Customer is a Processor of Personal Data, Sherweb shall process Personal Data as sub-processor on behalf of the Controller. Instructions from the Controller regarding the processing Personal Data shall be given through the Processor.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

“Personal Data” means any information relating to an identified or identifiable natural person (“Data Subject”).

“Processing/To Process/Processed” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
“Service Data” means all data provided to Sherweb, placed on Sherweb’s servers, or used, posted, stored or otherwise transferred or transmitted in connection with the Services, including text, sound, video or image file, material, product, content, IP address and similar address, recording, message, software, Account Information, account-related setting, and which may include, without limitation, Personal Data.

“Third Party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the Controller or Processor, are authorized to process Personal Data.

2. Scope of this Privacy Statement

This Privacy Statement governs our security and privacy practices in connection with your access to and use of Sherweb Services. This Privacy Statement does not apply to our security and privacy practices in connection with your access to and use of Sherweb’s website (www.sherweb.com). These security and privacy practices are detailed in and governed by Sherweb Privacy Policy.

Customers of our Services are solely responsible for establishing policies for and ensuring compliance with all applicable laws and regulations, as well as any and all privacy policies, agreements or other obligations, relating to the collection of personal data in connection with the use of our Services by Data Subjects with whom our Customers interact. If you are an individual who interacts with a Customer using our Services, then you will be directed to contact our Customer for assistance with any requests or questions relating to your personal data.

We collect information under the direction of our Customers and have no direct relationship with individuals whose personal data we process in connection with our Customers’ use of our Services. If you are an individual who interacts with a Customer using our Services (such as an employee of one of our Customers) and would either like to amend your contact information or no longer wish to be contacted by Sherweb, please contact the Customer that you interact with directly.

3. Data we Process

Sherweb may Process Personal Data about Data Subject for the purposes of account creation, billing, usage tracking, and on behalf Customer to provide the Services. Data that is not related to an identified or identifiable natural person, including aggregated or de-identified data, is not Personal Data and is not addressed by this document.

Types of Personal Data

Account Information
We may collect first and last name, email address, postal address, phone number and other similar contact data about Customer’s authorized employees, consultant or independent contractors.

Payment Data
We collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument.
Credentials
We collect passwords, password hints and similar security information used for authentication and account access.

Meta Data
Sherweb servers automatically record some information when Services are used, including information sent by browsers or mobile apps. Sherweb may collect information about the devices Services are being used on, including what type of device it is, operating systems, device settings, application IDs, unique device identifiers, and crash data.

Cookies and other Tracking Technologies
Whenever a Customer or any Account Users interact with the Portal, Sherweb automatically receives and records information from the browser, which may include IP address, “cookie” information, the type of browser and device being used to access the Portal, screen resolution and browser language. “Cookies” are identifiers Sherweb transfers to the browser or device of the Account User that allow Sherweb to recognize the Account User and their browser or device along with how our Portal is being utilized. When Sherweb collects this information, Sherweb only uses this data in aggregate form, and not in a manner that would identify the Account User personally. For example, this aggregate data can tell Sherweb how often users use a particular feature of the Portal, and Sherweb can use that knowledge to improve the Services. We also use an application session recording solution to record the Account Users’ use of the Portal and we may link such recordings to the Account User and the Customer Account to optimize our support services and better resolve technical problems. Such recordings are only used to provide technical support services under the Agreement.

Call Recording
Sherweb monitors and records calls to or from Sherweb regarding the Services, including Technical Support and account managers, for training, support, and quality control purposes.

Content
We process content of Customer’s files and communications when necessary to provide the Services. For example, if you receive an email using Hosted Exchange, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it and store it for you until you choose to delete it. Other data we collect to provide Services to Customer include the following:

- subject line and body of an email,
- text or other content of an instant message,
- audio and video recording of a video or audio message,
- audio recording and transcript of a voice message you receive or a text message you dictate, and
- Text or other content of a file or data Customer places on Sherweb’s servers, or uses, posts, stores or otherwise transfers or transmits in connection with the Services.

Voluntary Customer Surveys
We may periodically conduct both business and individual customer surveys. We encourage our Customers to participate in these surveys because they provide us with important information that helps us to improve the types of services we offer and how we provide them to you. Personal Data and responses submitted through these surveys will remain strictly confidential, even if the survey is conducted by a third party. Participation in our customer surveys is voluntary. We take
the information we receive from individuals responding to our customer surveys and combine (or aggregate) it with the responses of other customers to create broader, generic responses to the survey questions (such as gender, age, residence, hobbies, education, employment, industry sector, or other demographic information). We then use the aggregated information to improve the quality of our Services to you, and to develop new services and products. This data can be shared on an aggregate and anonymous basis with third parties.

4. Purposes for Processing

Sherweb processes the Personal Data outlined above for the following purposes:

- To operate our business;
- To provide and enhance our Services;
- To respond to Customer requests for support or assistance; and
- To send communications, including promotional communications.

This policy is not intended to place any limits on what we do with data that is aggregated and/or de-identified. It is no longer associated with an identifiable user or Customer of the Services and is therefore not Personal Data.

5. How we Protect Data

With regard to the Services and Service Data, Sherweb acts as a Processor on behalf of Customers. Customers have primary responsibility for interacting with Data Subjects, and the role of Sherweb is generally limited to assisting Customers as needed. Sherweb processes Service Data only upon a Customer’s instruction and shall have a duty to respect the security and confidentiality of Personal Data, pursuant to the measures outlined in agreements with Customers and as required by applicable law.

Information Security

Sherweb takes security seriously. We take various steps to protect Customer’s Service Data from loss, misuse, and unauthorized access or disclosure. These steps take into account the sensitivity of the Service Data, and the current state of technology.

Sherweb has a dedicated information security team consisting of an infrastructure team leader, infrastructure system administrators, and a senior security specialist, who are responsible for the management of information security throughout the organization. The specialist maintains security credentials and is required to annually sign and acknowledge the review of the information security policies. The specialist is responsible for developing, maintaining, and enforcing Sherweb’s information security policies. The information security policies are also reviewed annually by senior management.

In addition to maintaining security, the information security team also monitors known incidents and patches as well as results from vulnerability assessments; it makes changes to policies and procedures as needed following an approval process. Such changes can include the reassessment of risk, changes to incident response plans, and the verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly change maintenance meetings or through system alerts.
Sherweb implements and maintains a variety of technical and organizational security measures to protect Customer’s Service Data from loss, misuse, and unauthorized access or disclosure, including the following:

- Logical access controls to manage electronic access to data and system functionality based on authority levels and job functions (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).
- Password controls to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Sherweb’s passwords assigned to its employees: (i) be at least fourteen (14) characters in length, (ii) not be stored in readable format on Sherweb’s computer systems; (iii) must be changed every sixty (60) days; (iv) must have defined complexity; (v) may not be reused (password history); and (vi) newly issued passwords must be changed after first use.
- Housing systems in data center or server room facilities that are secured via physical and environmental controls that are designed to protect information assets from unauthorized access, to manage, monitor and log movement of persons into and out of Sherweb facilities, and to guard against environmental hazards such as fire and water damage.
- Operational procedures and controls to ensure technology and information systems are configured, monitored, and maintained according to prescribed internal and adopted industry standards.
- System logging procedures to proactively record user and system activity for routine review.
- Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and Intrusion Detection Systems and other traffic and event correlation procedures to protect systems from intrusion and limit the scope of any successful attack.
- Vulnerability management and scheduled scanning procedures and technologies to identify, assess, mitigate and protect against security threats, viruses and other malicious code.
- Change management procedures to ensure all changes to Sherweb’s technology and information assets are properly tested, approved and monitored.
- Incident / problem management procedures to allow for the proper investigation, response, mitigation and notification of events related to Sherweb’s technology and information assets.
- Organizational management to ensure the proper development and maintenance of information security and technology policies, procedures and standards.
- Audit and assessment procedures for the purposes of monitoring and maintaining compliance with the organization’s policies and procedures and for reporting the condition of information security to senior management.

**Personal Data Breach Notification**

In the event that Sherweb becomes aware of any of Security Incidents involving Personal Data, Sherweb will promptly notify affected Customers to the extent such notification is permitted by applicable law. “Security Incidents” are defined as (1) the actual unauthorized access to or use of unencrypted Personal Data by an unaffiliated third party, or (2) loss, theft, or unauthorized disclosure or manipulation of unencrypted Personal Data that has the potential to cause harm to
Customer’s systems, employees, information or the Customer’s brand name (i.e., potential breach).

Notification shall take the form of an email to the designated Customer Account Contact(s) and shall include at a minimum, (a) problem statement or description, (2) expected resolution time (if known), and (b) the name and phone number of the Sherweb representative that Customer may contact to obtain updates.

Sherweb agrees to keep Customer informed of progress and actions taken to resolve the Security Incident. Unless such disclosure or notification is mandated by law, Customer, in its sole discretion, will determine whether to provide explicit notification to Customer’s customers or employees concerning Security Incidents involving Personal Data. Sherweb reserves the right, in its sole discretion, to notify pertinent government authorities of such incidents, such as those involving criminal acts.

6. Transparency and Cooperation with Customers

Sherweb undertakes to be transparent regarding its Personal Data processing activities and to provide Customers with reasonable cooperation to help facilitate their respective data protection obligations regarding Personal Data.

Upon a Customer’s request, and subject to appropriate confidentiality obligations, Sherweb shall make available to the Customer (or such Customer’s independent, third-party auditor) information regarding Sherweb processing activities affecting Customer.

7. Sharing and Disclosure

This section discusses how Sherweb may share Personal Data with third-parties in the context of the Services.

Sherweb reserves the right to disclose or use aggregate or de-identified information for any purpose. For example, we may share aggregated or de-identified information with our partners or others for business or research purposes.

Sub-processing by Third Parties
Sherweb may retain third party sub-processors, and depending on the location of the third-party sub-processor, processing of Personal Data by such sub-processors may involve transfers of Personal Data. Such third-party sub-processors shall process Personal Data only in accordance with the Customer’s instructions set forth in the Customer’s contract with Sherweb.

Such third-party sub-processors have entered into written agreements with Sherweb in accordance with the applicable requirements. Sherweb maintains an up-to-date list of the names and locations of all third-party sub-processors engaged in processing Personal Data, including a description of their processing activities, which is available upon request by contacting privacy@sherweb.com.

Compliance with Laws
Sherweb may share or disclose data to comply with legal or regulatory requirements and to respond to lawful requests, court orders and legal processes.
Enforcing Our Rights, Preventing Fraud, and Safety
Sherweb may share or disclose data to protect and defend the rights, property, or safety of us or third parties, including enforcing contracts or policies, or in connection with investigation and preventing fraud.

Changes to our Business Structure
Sherweb may share or disclose data if we engage in a merger, acquisition, bankruptcy, dissolution, reorganization, sale of some or all of Sherweb’s assets, financing, acquisition of all or a portion of our business, a similar transaction or proceeding, or steps in contemplation of such activities (e.g. due diligence).

8. Location of Data
The Service Data is hosted on Sherweb’s servers located in data centers in the United States and Canada. Default location is based on Customer location and can be modified by Customer once the Services are provisioned, subject to applicable fees.

9. Personal Data Retention
We will retain Personal Data for as long as Customer maintains an Account for our Services, or as needed to provide Customer with our Services, comply with our legal obligations, resolve disputes and enforce our agreements. If we have no ongoing legitimate business need to process or retain Personal Data, we will either delete or anonymize it, or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will securely store your data and isolate it from any further processing until deletion is possible.

10. Data Subject Rights
Sherweb acts as a data Processor on behalf of Customers. Customers have primary responsibility for interacting with Data Subjects, and the role of Sherweb is generally limited to assisting Customers as needed.

Access, Correction, Amendment or Deletion Requests
Sherweb shall promptly notify a Customer if Sherweb receives a request from a Data Subject for access to, correction, amendment or deletion of that person’s Personal Data. Sherweb shall not respond to any such Data Subject request without the Customer’s prior written consent except to confirm that the request relates to that Customer.

Sherweb shall provide Customers with cooperation and assistance in a reasonable period of time and to the extent reasonably possible in relation to any request regarding Personal Data to the extent Customers do not have access to such Personal Data through their respective uses of the Services.

Customers may update or change their Account Information by editing their profile or organization record directly on the Portal.
If you are a Customer or otherwise provide us with personal data in connection with your use of our Services, we will delete this information upon your request, provided that, notwithstanding such request, this information may be retained for as long as you maintain an Account for our Services, or as needed to provide you with our Services, comply with our legal obligations, resolve disputes and enforce our agreements.

**Regulatory Enquiries and Complaints**
Sherweb shall, to the extent legally permitted, promptly notify a Customer if it receives an enquiry or complaint from a data protection authority in which that Customer is specifically named. Upon a Customer’s request, Sherweb shall provide the Customer with cooperation and assistance in relation to any regulatory inquiry or complaint involving Sherweb’s processing of Personal Data.

**Legal Requests**
In certain situations, Sherweb may be required to disclose Service Data in response to lawful requests by public authorities, to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. Sherweb may also share such information with relevant law enforcement agencies or public authorities if we believe same to be necessary in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Master Subscription Agreement, or as otherwise required by law.

11. **Changes to this Statement**
We may change this statement from time to time, and if we do we will post any changes on this page. If you continue to use the Services after those changes are in effect, you agree to the revised policy.

12. **How to Contact Sherweb**
Please feel free to contact us if you have any questions about Sherweb’s Privacy commitments or practices. You may contact us at privacy@sherweb.com or at our mailing address below:

SHERWEB INC.
Attn: Director, Legal – Contracts and Compliance
95 South Jacques-Cartier Blvd, Suite 400
Sherbooke (QC) Canada
J1J 2Z3
Email: privacy@sherweb.com