

Privacy Policy

(Effective January 7, 2026)

Welcome!

Welcome to Nectari! We hope that you will enjoy and appreciate using our “**Services**”, which may include: (i) visiting the website at <https://www.nectari.com/> or any subdomain thereof, including <https://academy.nectari.com/>, <https://notifications.nectari.com/> and <https://status.nectari.com/> (the “**Website**”); (ii) using the client portal accessible from the Website to consult resources for the Nectari software and your invoicing and payment dashboard (the “**Client Portal**”); (iii) using the e-learning portal at <https://academy.nectari.com/> to access Nectari e-learning resources (the “**e-Learning Portal**” and, together with the Client Portal, the “**Portals**”); or (iv) receiving access to Nectari’s cloud hosting services and the cloud-based version of the Nectari software (the “**SaaS Software**”).

Nectari Software Inc., the company that owns and operates the Services, wants you to know that we take your privacy and the protection of personal data very seriously. We are providing this Privacy Policy (the “**Policy**”) to tell you about who we are, what personal data we collect from you and about you, and what we do with your personal data, all while you use the Services or otherwise interact with us online. The Policy also explains your rights under applicable law, and how you can contact us and the necessary authorities to enforce those rights. We ask that you please read it carefully.

Key Elements of this Policy

Here are the key elements of this Policy so that you can know the important parts right away to make an informed decision about your consent for our collection, use and disclosure of your personal data. By submitting any personal data to us via any means, you consent to such collection, use and disclosure. You can find the details in the rest of the Policy.

Personal data we collect from you but only with your consent:

Contact Information

- What we do with it: Communicate with you and manage our relationship, depending on your relationship with us
- Third parties we share it with: Companies that provide our communications services, such as HubSpot and Better Stack

Client Portal Account Information

- What we do with it: Manage your Client Portal account, and enable logging into the Client Portal
- Third parties we share it with: Odoo, the company that provides the infrastructure for the Website and the Client Portal; Beamer, a company that provides email updates about our SaaS Software

e-Learning Portal Account Information

- What we do with it: Manage your e-Learning Portal account and enable logging into the e-Learning Portal
- Third parties we share it with: LearnWorlds, our learning management system service provider

SaaS Software Account Information

- What we do with it: Manage your account and enable logging into the SaaS Software; configure and deploy your cloud environment
- Third parties we share it with: Microsoft Azure, the company that provides the infrastructure for the SaaS Software; your SaaS Software reseller/partner/sales agent, if applicable

SaaS Software Inputs

- What we do with it: Share it with our third-party artificial intelligence (“AI”) provider, in order to process your inputs and produce the requested outputs, all within the SaaS Software
- Third parties we share it with: Microsoft Azure, the company that provides the infrastructure for the SaaS Software and the SaaS Software’s AI features

Payment Information

- What we do with it: Permit you to pay for any of our Services (via the SaaS Software, the Client Portal or the e-Learning Portal), including any optional add-ons or usage-based services (such as AI credits and additional cloud hosting options)
- Third parties we share it with: Stripe, our payment processor

Some Terms

Before we get started with the details, here are a few terms we think you should know as you read this Policy.

“**Data Protection Laws**” refers to the laws that are designed to protect your personal data and privacy in the place where you live. Nectari is committed to adhering to all applicable Data Protection laws. The Data Protection Laws include: (1) the “**GDPR**”, the European Data Protection Law which stands for “General Data Protection Regulation”, with the official name *Regulation (EU) 2016/679 of the European Parliament and of the Council*; (2) the “**UK GDPR**” which applies to our activities in the United Kingdom; please note that when this Policy refers only to the “GDPR”, this includes the UK GDPR as applicable; (3) “**PIPEDA**” (*Personal Information Protection and Electronic Documents Act*), which is the Canadian Data Protection Law that applies to our activities in Canada; and (4) Quebec’s *Act Respecting the Protection of Personal Information in the Private Sector* (the “**Quebec Privacy Act**”) as amended by Law 25, that applies to our activities in Quebec.

“**Personal data**” – this is information that we collect from you or about you and which is defined in the GDPR as “any information relating to an identified or identifiable natural person.” It can be as simple as your name or your email, or something more complicated like an online identifier (usually a string of letters and / or numbers) that gets attached to you. Under PIPEDA and the Quebec Privacy Act, the equivalent concept is “personal information”, which is roughly the same. For example, the Quebec Privacy Act defines “personal information” as “any information which relates to a natural person and allows that person to be identified either directly or indirectly.” Any mention of “personal data” in this Policy will also mean personal information.

Other terms and definitions used in this Policy may be found in our [Terms of Use](#) and will have the same meaning in this Policy as they do there.

About Us and Contacting Us

Nectari Software Inc. (“**Nectari**”) is a duly incorporated company in the province of Quebec, Canada that owns and operates the Services. Where this Policy refers to “Nectari”, it may refer to Nectari Software Inc. and / or its shareholders, officers, directors, employees, agents, partners, principals, affiliates, representatives, successors and assigns, depending on the context.

Under the GDPR, Nectari Software Inc. is a “data controller”. That means we collect personal data directly from you and determine the purpose and means of “processing” that data. “Processing” is a broad term that means the collection, use, storage, transfer or any other action related to your personal data; it is used in this Policy in that way. Under PIPEDA, Nectari is an “organization”, and under the Quebec Privacy Act, Nectari is an “enterprise”. PIPEDA uses the phrase “collection, use and disclosure” and the Quebec Privacy Act uses the phrase “collects, holds, uses or communicates to third parties” as the rough equivalent to the “processing” of the GDPR. When we use “processing” in this Policy, you can substitute either of those phrases.

If you want to ask us anything about what’s in this Policy, or anything else privacy- or data- related, or exercise any of your available privacy rights, you can contact:

Nectari Privacy and Data Protection Officer
privacy@nectari.com

Here is the mailing address for you as well:

Nectari Privacy and Data Protection Officer
1120-400 Sainte-Croix Avenue
Montréal, Québec
H4N 3L4, Canada

Your Rights

You have the following rights regarding your personal data held by Nectari, and other privacy rights. Please note that not necessarily all of these rights may be available to you; this depends on the Data Protection Laws where you are located that apply to you. These rights may be exercised without affecting the price you pay for any of the Services. Notwithstanding that, exercising certain of these rights may affect your ability to use some or all of the Services.

- The right to withdraw at any time your consent for Nectari to process your personal data;
- The right to have your personal data erased from Nectari’s records;
- The right to have a link removed from Nectari’s Website or Portals that is associated with your name;
- The right to access your personal data and any relevant information around its processing and use;
- The right to have a copy of your personal data given to you in an easy to read format so that you can transfer it to another organization;
- The right to have your personal data corrected or updated if you believe it is inaccurate or out of date;

- The right to opt out of marketing communications we send you, at any time;
- The right to know whether Nectari sells or shares your personal data (and if so, who gets it). Please refer to that information elsewhere in this Policy, though you can contact our Privacy and Data Protection Officer if you need additional information or clarification;
- The right to demand that Nectari not sell your personal data. Please note that Nectari does not sell your personal data;
- The right to restrict the processing of your personal data if it is inaccurate or if our processing or use of it is against the law; and
- The right to refuse any marketing or advertising targeted at you by Nectari.

If you wish to exercise any of these rights, please contact our Privacy and Data Protection Officer at the contact information above or refer to certain relevant sections further in this Policy.

Please note that if you request the erasure of your personal data, we will do so to the extent possible. However, Nectari reserves the right to retain certain data for a reasonable period of time in order to comply with certain legal obligations or for the purposes of any legal proceedings.

Limited Personal Data Collected from You and What We Use It For

Nectari limits the amount of personal data we collect to what is necessary and appropriate for the identified purposes. We will not use or disclose your personal data for purposes other than those for which it was collected, except with your consent or as permitted or required by applicable law.

Here are all the personal data we may collect from you directly, what we use it for, and the legal basis under the GDPR for us having and processing this personal data. Under PIPEDA and the Quebec Privacy Act, the legal basis is your informed consent, and by submitting this personal data to us, you acknowledge having granted this consent to Nectari.

Contact Information

- Personal data processed: Name, email address, the company that you work for and the country or region where you are located
- What we use it for (the “purpose” of processing): To communicate with you in response to a request to join our mailing list or to seek additional information from us
- Legal basis for processing under the GDPR: Your consent in giving us this information

Client Portal Account Information

- Personal data processed: Name, email address and the company that you work for
- What we use it for (the “purpose” of processing): To manage your Client Portal account, give you access to all of our Client Portal features and enable logging in to the Client Portal
- Legal basis for processing under the GDPR: Your consent in giving us this information and the performance of a contract between you and us

e-Learning Portal Account Information

- Personal data processed: Name and email address and, optionally, the country where you live, your professional experience, a photo of yourself and links to your social media accounts
- What we use it for (the “purpose” of processing): To manage your e-Learning Portal account, give you access to all of our e-Learning Portal features and enable logging in to the e-Learning Portal

- Legal basis for processing under the GDPR: Your consent in giving us this information and the performance of a contract between you and us

SaaS Software Account Information

- Personal data processed: Name and email address
- What we use it for (the “purpose” of processing): To manage your SaaS Software account and enable logging into the SaaS Software; to configure and deploy your cloud environment
- Legal basis for processing under the GDPR: Your consent in giving us this information and the performance of a contract between you and us

SaaS Software Inputs

- Personal data processed: Any personal data that you submit to the SaaS Software as an input (but not your SaaS Software Account Information)
- What we use it for (the “purpose” of processing): To share with our third-party AI provider, in order to process your inputs and produce the requested outputs, all within the SaaS Software
- Legal basis for processing under the GDPR: Your consent in giving us this information

Payment Information

- Personal data processed: Credit card number, credit card expiry date, credit card security code (CVV) and billing address
- What we use it for (the “purpose” of processing): To permit you to pay for any of our Services (via the SaaS Software, the Client Portal or the e-Learning Portal), including any optional add-ons or usage-based services (such as AI credits and additional cloud hosting options)
- Legal basis for processing under the GDPR: Your consent in giving us this information and the performance of a contract between you and us

If you happen to share or communicate personal data with us other than as explicitly set forth in this Policy, we will treat any such personal data in accordance with this Policy.

Where you have provided personal data further to the contract between you and us, if you fail to provide such data or withdraw your consent to use such data, we will no longer be able to provide certain Services to you.

Personal Data Collected About You from Third Parties and What We Use It For

We sometimes obtain personal data about you from third parties, or third parties collect it on our behalf and use it. The following section explains the details about this personal data – what it is, where it came from, what we do with it, and the legal basis for us having and processing this personal data under the GDPR. Under PIPEDA and the Quebec Privacy Act, the legal basis for our collection, use and disclosure of this personal data is your informed consent, and by submitting this personal data to third parties, you acknowledge that you have given such consent. None of this data comes from publicly available sources.

Contact Information

- Personal data processed: Your name and email address; your responses to survey questions
- Who we get the data from: Jotform, the service provider that we use to share surveys with customers or to integrate surveys into our newsletters

- What we use it for (the “purpose” of processing): To process your survey responses and to improve the Services
- Legal basis for processing under the GDPR: Your consent

SaaS Software Account Information

- Personal data processed: Your name and email address
- Who we get the data from: Your SaaS Software reseller/partner/sales agent or another user from your company or organization that has an admin-level account and invites other users to access the SaaS Software
- What we use it for (the “purpose” of processing): To manage your SaaS Software account and to enable logging into the SaaS Software; to configure and deploy your cloud environment
- Legal basis for processing under the GDPR: Our legitimate business interests

In addition, to the extent that analytics identifiers are generated from third parties or collected from any third party, these may be considered personal data collected from third parties and you can find details about those further below in this Policy.

Sensitive Personal Data

We do not collect any of what the Data Protection Laws consider sensitive personal information from you, unless you voluntarily submit it to us via the Services, which we encourage you not to do.

Who We Transfer Your Personal Data To

We only share some of your personal data with third parties who are identified below in this section, along with what they do with it. Each type of third party identified below is under a contractual obligation not to (1) transfer or sell your personal data; or (2) use your personal data for any purpose, other than the purpose identified in the table below.

We will share personal data with law enforcement or other public authorities if: (1) we are required by applicable law in response to lawful requests, including to meet national security or law enforcement requirements; (2) we believe it is necessary in order to investigate, prevent, or take action regarding illegal activities, fraud, or situations involving potential threats to the safety of any person; (3) we believe it is necessary to investigate, prevent, or take action regarding situations that involve abuse of the Website or the Services infrastructure or the Internet in general (such as voluminous spamming or denial of service attacks); or (4) we are required to under any applicable law.

We may also share personal data: (1) to a parent company, subsidiaries, joint ventures, or other companies under common control with Nectari (in which case we will require such entities to honour this Policy); (2) if Nectari merges with another entity, is subject to a corporate reorganization, sells or transfers all or part of its business, assets or shares (in which case, we will require such entity to assume our obligations under this Policy, or inform you that you are covered by a new privacy policy).

Some of these third-party recipients may be based outside your home jurisdiction. If you are in the European Economic Area or the U.K., please see the “Transfer of Your Personal Data Outside of the European Economic Area and the U.K.” further down in this Policy for more information, including on how we safeguard your personal data when this occurs. If you are in Quebec, please see the “Transfer of Your

Personal Data Outside of Quebec” section further down in this Policy for information on how we safeguard your personal data when this occurs.

We will never share your personal data with other third parties except under these circumstances, or as otherwise permitted under applicable Data Protection Laws. We do not sell or rent your personal data to any third party for direct marketing purposes or any other purpose.

Contact Information

- Who we transfer it to: Companies that provide email services, specifically [HubSpot](#), as detailed more fully in the “Email Communications” section below; [Better Stack](#), our incident management platform service provider
- What they do with it: Send you emails on our behalf; send you emails with status updates, if you sign up for updates at <https://status.nectari.com/>

Client Portal Account Information

- Who we transfer it to: Companies providing technical infrastructure for the Client Portal, specifically [Odoo](#); [Beamer](#), a company that provides email updates about our SaaS Software (if you sign up for email updates at <https://notifications.nectari.com/>)
- What they do with it: Store it; control your logging into the Client Portal and enable your access thereto; send you email updates about our SaaS Software

e-Learning Portal Account Information

- Who we transfer it to: Our learning management system service provider, [LearnWorlds](#)
- What they do with it: Store it; control your logging into the e-Learning Portal; save and present you with your Nectari training course history and certifications

SaaS Software Account Information

- Who we transfer it to: Companies providing the technical infrastructure for the SaaS Software, specifically [Microsoft Azure](#); your SaaS Services reseller/partner/sales agent
- What they do with it: Store it, control your logging in to the SaaS Software and enable your access thereto, record-keeping purposes; communicate with you, manage your access to the SaaS Software and provide you with implementation and support services for the SaaS Software

SaaS Software Inputs

- Who we transfer it to: [Microsoft Azure](#), our third-party AI provider
- What they do with it: Process your inputs and produce the requested outputs, all within the SaaS Software

Payment Information

- Who we transfer it to: [Stripe](#), our payment processor; companies providing technical infrastructure for the Client Portal, specifically [Odoo](#)
- What they do with it: Process your payment for any of our Services, including any optional add-ons or usage-based services (such as AI credits and additional cloud hosting options); store your payment history within your Client Portal account

Analytics Identifiers (including IP addresses)

- Who we transfer it to: Companies that provide data analytics, specifically [Google Analytics](#)

- What they do with it: Provide us with analytics as to how the Services are used and to trace fraudulent activities

Limited Gathering of Information for Statistical, Analytical and Security Purposes

Nectari automatically collects certain information using the “**Third-Party Analytics Program**” from Google Analytics to help us understand more about our Website visitors and customers and how they use the Website and the Services, but none of this information identifies you personally, except via an alphanumeric string. For example, each time you visit the Website or the Portals, we automatically collect (as applicable) your IP address, browser and computer or device type, access times, the web page from which you came, the web page(s) or content you access, and other related information. We use information collected in this manner only to better understand your needs and the needs of Website visitors and customers in the aggregate. Nectari also makes use of information gathered for statistical purposes to keep track of the number of visits to the Website and the Portals, the specific pages visited on the Website and the Portals and the number of Website and Portal visitors, with a view to introducing improvements to the Website, the Portals and our marketing activities.

Your IP address and other relevant information we collect using the Third-Party Analytics Program may also be used in order to trace any fraudulent or criminal activity.

Tracking Technology (“Cookies”) and Related Technologies

Nectari uses tracking technology (“cookies” and related technology such as tags, pixels and web beacons) in connection with the Services and by interacting with the Services you agree to their use. Cookies are small text files placed on your computer or device when you visit a website or use an online service, in order to track use of the site or service and to improve the user experience by storing certain data on your computer or device. More specifically with respect to emails, HubSpot uses pixels in the emails that it sends on our behalf in order to determine whether you open an email that you receive from us and whether you click on any links included in the email. By visiting the Website or the Portals, you agree to the use of cookies and related technologies, but only if you explicitly consent to such use, according to the cookie banner presented to you when you visit the Website or the Portals. By default, all non-essential cookies are turned off when you first visit the Website and the Portals – you can use our cookie management tool to accept or decline all other categories of cookies.

Specifically, we use cookies and related technologies for the following functions:

- for the proper functioning of the Website and the Portals;
- to provide general internal and user analytics on the Website and the Portals and to improve the content of the Website and the Portals using Google Analytics as listed above in this Policy;
- to track information about emails you receive, for example, whether you opened it or clicked on any links in it; and
- to assist in identifying possible fraudulent activities.

Your browser can be set to refuse cookies or delete them after they have been accepted and stored. You can refer to your browser’s help section for instructions, but here are instructions for the most commonly used browsers and operating systems:

- [Google Chrome](#)
- [Mozilla Firefox](#)
- [Microsoft Edge](#)
- [Opera](#)
- [Apple Safari](#)
- [iOS](#)
- [Android](#)

Please note that deleting or blocking certain cookies may reduce your user experience by requiring you to re-enter certain information, including information required to use our Services.

Email Communications and Compliance with Anti-Spam Laws

Nectari uses HubSpot to manage our mailing list and to send out promotional emails (the “**Email Service Provider**”). Personal data is transferred to the Email Service Provider in order to manage the mailing list and for the emails to be sent out properly. Your email address is only used to send out emails; the Email Service Provider does not use this personal data for any other purpose and will not transfer or sell your personal data to any other third party. For more information, please refer to [HubSpot's Privacy Policy](#).

You may unsubscribe from Nectari’s mailing list at any time by following the link at the bottom of our newsletter. Other types of emails, such as transactional, relational and other emails related to the Services will not have an opt-out option as they are necessary for the use of the Services.

Nectari’s practices with respect to its email are designed to be strictly compliant with anti-spam laws, specifically the law unofficially called “**CASL**”, or Canada’s Anti-Spam Law (S.C. 2010, c. 23). If you believe you have received email in violation of these laws, please contact our Privacy and Data Protection Officer using the contact information further up in this Policy.

How We Protect Your Personal Data

We have implemented strict technical and organisational procedures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed by us. These procedures prevent your personal data from being lost; or used or accessed in any unauthorised way.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable supervisory authority of a suspected data security breach where the Data Protection Laws require us to do so, and within the time frame required by the applicable Data Protection Law.

Nectari uses only industry best practices (physical, electronic and procedural) in keeping any data collected (including personal data) secure. In addition, we use third-party vendors and hosting partners to provide the necessary hardware, software, networking, storage, and related technology required to operate the Services, and these third parties have been selected for their high standards of security, both electronic and physical. For example, Nectari uses [Odoo](#) for hosting of the Website and the Client Portal and [Microsoft Azure](#) for hosting of the SaaS Software and all related data. Each of Odoo and Microsoft Azure have robust security programs – for more information about Odoo’s program, please click [here](#) and [here](#) and for Microsoft Azure’s program, please click [here](#) and [here](#).

All information, including personal data, is transferred with encryption using Secure Sockets Layer (“SSL”) or Transport Layer Security (“TLS”), robust security standards for Internet data transfer and transactions. You can use your browser to check Nectari’s valid SSL security certificate.

Internal Procedures and Policies

In addition to the measures to protect your personal data described in the previous section, we have drafted and implemented certain internal procedures and policies regarding personal data, including the following:

1. A framework for the keeping and destruction of the personal data that we collect, including where we may keep anonymized data;
2. Defining and describing the roles and responsibilities of the members of Nectari personnel throughout the life cycle of the personal data;
3. A process for dealing with individual complaints and requests for personal data and exercising of an individual’s rights under Data Protection Laws; and
4. A management and IT policy and procedure for addressing potential data breach incidents involving personal data in the custody of Nectari.

Transfer of Your Personal Data Outside of the European Economic Area (“EEA”) and the UK

For our European Website visitors and customers, we endeavour to keep your personal data inside the EEA or the U.K. (as applicable).

Certain of our data processors (and Nectari) are in other countries where your personal data may be transferred. However, these countries are limited to countries with particular circumstances that protect your data, specifically:

- Canada. We transfer personal data to our operations in Canada, but Canada has been determined to have an “adequate level of protection” for your personal data [under European Data Protection Laws](#).
- The United States. Your personal data is only transferred to companies in the United States that: (1) have signed agreements with us or have informed us that they are GDPR-compliant; and (2) have concluded the [Standard Contractual Clauses](#) for the transfer of personal data outside the EEA and the U.K.

That’s it! You have the right, however, to refuse to have your data transferred outside the EEA or the UK. Please contact our Privacy and Data Protection Officer to make that request. Please note that making this request may prevent you from being able to use a portion or all of the Services.

Transfer of Your Personal Data Outside of Quebec

For our Quebec Website visitors and customers, we endeavour to keep your personal data in Quebec. However, certain of our third-party service providers are in other provinces or countries where your

personal data may be transferred. When this happens, we do the following to safeguard your personal data:

1. We will perform what the Quebec Privacy Act calls an “Assessment of the privacy-related factors” (what is generally called a “Privacy Impact Assessment,” or “PIA”) prior to the personal data leaving Quebec. If the PIA does not meet our standards and the standards required by the Quebec Privacy Act, we will not transfer your personal data to such a service provider; and
2. If the PIA allows us to transfer the personal data to such a service provider outside Quebec, we will sign what is generally called a “Data Processing Agreement,” or DPA, with the service provider, which protects the personal data transferred to them and limits their use of it to what we have contracted with them to do. This DPA will adhere to the requirements of the Quebec Privacy Act.

Supervisory Authorities and Complaints

If you are in the EEA or the UK, under the GDPR you have the right to make a complaint to the appropriate supervisory authority. If you are not satisfied with the response received or the actions taken by our Privacy and Data Protection Officer, or if you would like to make a complaint directly about Nectari’s data practices, we invite you to contact the supervisory authority in your country. For example, if you are in the U.K., you should contact the Information Commissioner’s Office who is the supervisory authority. You can [reach them in a variety of ways](#), including by phone (0303 123 1113 in the UK) and mail (Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF). If you are in France, you should contact the *Commission Nationale de l’Informatique et des Libertés*, which is the supervisory authority there. Their contact information [can be found here](#).

The full listing of all Data Protection Authorities (the supervisory authorities) across the EEA [can be found here](#).

If you are in Canada and you are not satisfied with the response received or the actions taken by our Privacy and Data Protection Officer, you can make a complaint to the Office of the Privacy Commissioner of Canada. Instructions on how to do so can be found on their [website](#). In Québec you can make a complaint to the *Commission d’accès à l’information*, with the instructions for contacting them on their [website](#).

Data Retention

Your personal data will only be kept for as long as it is necessary for the purpose needed for that processing. For example, we will only retain your Client Portal Account Information, e-Learning Account Information or SaaS Software Account Information for as long as you have an account with us.

We may have to keep your data for a longer period of time to satisfy our requirements under any applicable law, including anti-spam laws, or to protect our legal interests.

In some cases, where permitted by the Data Protection Laws, we may keep personal data that has been anonymized, for our legitimate business purposes.

Automated Decision-Making

Nectari does not use any automated decision-making processes regarding your personal data in providing the Services.

Children's Privacy Statement

The Services are only intended for persons who are 18 years old for a resident of a Canadian province or the age of majority in any other country.

The Data Protection Laws have various age limits as to the minimum age required for us to hold personal data about an individual. We do not knowingly collect any personal data from a child under those minimum ages. If we become aware that we have inadvertently received personal data from a person under the minimum ages through the Website or Services, we will delete such information from our records.

Changes to This Privacy Policy

The date at the top of this page indicates when this Policy was last updated. Because Data Protection Laws are constantly evolving, every now and then we will have to update this Policy. You can always find the most updated version at this URL. If we make significant changes to the Policy, we will always post a notice on the Website and contact you if you are a customer.

© Nectari Software Inc., 2026