

Effective/Last Updated: 1 May 2026

BNI New Zealand Limited Privacy Policy

BNI New Zealand Limited ('BNI NZ') knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. We are committed to ensuring that your privacy is protected. This Privacy Policy describes how we deal with your personal information, who we disclose it to and how you may be able to access and correct the personal information we hold about you.

By visiting the BNI NZ Website - [New Zealand](#), you are accepting the practices described in this Privacy Policy. We encourage you to read this Policy carefully when using our Sites or transacting business with us.

What Personal Data is Being Collected

We collect the following categories of personal data about you either directly from you or indirectly from third parties (as applicable):

- **Identification & Contact Data** such as your name, username, business or home address, email address, phone number, account credentials and identity documents (e.g., passport or driver's licence) used to create or manage an account.
- **Membership & Chapter Participation Data** such as the Chapter(s) you are affiliated with and your role within those Chapter(s), attendance records, records of referral, membership status, the name of the member who invited you (where applicable), your business details such as your profession and area of expertise, and other details about your membership or attendance in a Chapter or Chapter meeting.
- **Transaction & Account Data** including purchase and subscription records, billing confirmations from our payment processor (we do not store full card numbers), and your in-product settings or preferences.
- **Usage & Technical Data** generated when you use our Sites, apps, or AI-powered features, including device and browser identifiers, IP-based approximate location, pages viewed, links clicked, session length, performance and crash diagnostics, and basic attribution (for example, which campaign link brought you to our site).
- **Communications Data** contained in messages you send to us (support requests, feedback, surveys) and content you post through our services (for instance, a profile photo or short video).
- **Special Category / Sensitive Data** only where you choose to provide it or where a specific feature requires it—such as health or biometric information, precise geolocation, financial account details, or information about minors. We collect and use this category only with an appropriate legal basis (including explicit or separate consent where required under applicable laws).

You are not required to provide special category or sensitive personal data to use most of our services. However, if you decline to provide such data or consent to its processing, certain features or functions of our services may not be available.

Ways in Which We Collect Your Personal Data

We may collect personal data from a variety of sources. This includes:

- **Directly from you.** You provide information when you register, purchase, complete a form or survey, upload content, contact or communicate with us (including for support). This can include your contact details and login information; profile fields you choose to add (such as role, age group, or preferred pronouns); the text, prompts, or files you submit to AI features so those features function; and any attachments you upload. For payments, we receive processor-issued tokens or confirmations, not full card numbers. In limited cases— only if you supply it—we may process your own professional revenue figures; most revenue data we handle relates to organizations rather than an identifiable person.
- **Automatically from your device/use.** When you visit our Sites or apps, we receive technical and usage signals your device or browser ordinarily shares, such as IP address (which indicates an approximate location), device and browser type, operating system and language, referral and exit pages, timestamps, pages viewed, links selected, session duration, load times, search terms, and crash/error diagnostics. If you interact with AI features, we process the inputs you provide so the feature works as intended.
- **Cookies and similar technologies (consent where required under applicable laws).** We use cookies, SDKs, and pixels to keep you signed in, remember settings like language, secure the service, and understand what is working. Our emails may include simple beacons so we can gauge opens or link clicks and avoid unnecessary resends. You can manage nonessential cookies in our banner or your browser; some features may not function without them. To the extent you disable cookies by refusing them through turning them off in your browser and/or deleting them from your hard drive, your access to some of the Sites' content and features may be limited. While you do not need to have cookies turned on to use our Sites, your experience may be affected.
- **From other people and trusted partners.** A colleague, customer/client, employee or member may share your business contact details or other personal data set out in this Policy to invite you to an event, meeting or make a referral (about you or to you); the person sharing should have a lawful basis and, where required by applicable laws, direct you to this policy. We also receive data from providers who help with operations and safety—such as address corrections from shippers, billing confirmations from payment processors, fraud-prevention risk signals, analytics or attribution aggregates about feature usage or campaign performance, customer-support tooling, and, where appropriate, public sources (for example, company registries) to validate business details. Where legally permitted and necessary (for fraud prevention, assessing eligibility for a financing option or otherwise), we may obtain limited credit-reference information. If you join through or participate in a partner program, benefit offering, or co-sponsored program, we may receive information from the relevant partner organization to verify eligibility, administer the program, or maintain accurate records.
- **From service providers and third-party affiliates or contractors to us.** We may receive personal information about you from service providers and third-party affiliates or contractors of us if it is reasonably necessary for service providers and third-party affiliates or contractors to carry out their duties in accordance with their contractual obligations.
- **Publicly available sources.** Personal data may be obtained from public registers, government agency publications, news articles, sanctions lists, internet searches and social media sites in order to carry out background checks or as part of the normal course of our provision of services.
- **Combining information.** Where the law allows, we combine information from these sources—such as merging duplicate accounts, troubleshooting issues, enhancing security, keeping records accurate, or improving service quality.

You may decide not to provide your personal data to us. However, if you do not provide it, we may not be able to provide you with the services you have requested or access to the Sites or certain parts of the Sites, or you may not be able to fully utilize all our services.

When and Why We Collect Special Category / Sensitive Data

We do not require sensitive or special-category data for core services. If you choose to share such data—including via optional AI features—we will process it only in accordance with applicable laws, for example, with an appropriate legal basis and for the specific purpose disclosed at collection (for example, explicit consent under GDPR Article 9(2) or separate consent under PIPL for sensitive personal information). If you withhold consent for these items, only the related optional feature will be unavailable; other features will continue to work.

What Purpose Do We Use Your Data For?

We use personal data to provide and improve our services. Depending on what you're doing and our requirements under applicable laws, we may rely on your **consent**, our **contract** with you, or our **legitimate interests**. Where the law requires consent (for example where applicable, for non-essential cookies, certain marketing, or sensitive/special-category data), we will ask first. You may withdraw consent at any time; withdrawing won't affect processing already carried out.

Processing with your consent: To the extent your consent is required under applicable laws, with your permission we may: remember your settings and measure use through non-essential cookies/SDKs; send marketing communications (including emails), newsletters or product updates; allow business partners, GPO partners, or co-sponsored program partners to contact you directly about their offerings where you have provided consent; run surveys or record certain optional interactions; and collect or use sensitive/special-category data you choose to share (such as health, biometric or precise location data) for a clearly stated purpose. If you use AI features, we process the text, prompts, or files you submit to enable the feature to work. To the extent required under applicable laws, we will not use your personal data to train or improve AI models unless you provide explicit (GDPR) / separate (PIPL) consent for that specific use. Under PIPL (where applicable), we also request separate consent for cross-border transfers where required, and provide an opt-out of personalized recommendations.

Processing necessary to perform our contract with you: To deliver our services, we may create and manage your account, authenticate logins, and provide core platform features (including networking tools, member directories, referral tracking, chapter management, event and training management, performance analytics, and AI-powered features you choose to use). We process orders and subscriptions, communicate with you, monitor website and application usage, and provide customer support.

For payments, we rely on a payment processor and receive tokens, confirmations, and receipts; we do not store full card numbers. We send service and transactional messages—such as receipts, account or security notices, feature changes, and policy updates—so you can use the product you purchased.

We may also use personal data to administer partner programs, verify eligibility for partner-related benefits, facilitate member benefit programs you elect to participate in, and support participation tracking, notifications, and related member activities.

Processing based on our legitimate interests: We also process personal data to keep the service secure and useful. This includes protecting accounts and our Sites (fraud detection, abuse prevention, rate-limiting suspicious traffic), troubleshooting and improving performance (telemetry, crash diagnostics, load-time

monitoring), understanding how features are used so we can improve them, and managing relationships (handling referrals or event invitations that others send you, maintaining accurate records, and de-duplicating accounts). In B2B contexts, we may send product news about similar services to existing customers under a soft-opt-in where permitted; you can opt out at any time. Where ePrivacy or local law requires consent (for example, for certain cookies or direct marketing), we rely on consent instead of legitimate interests.

Compliance and legal duties: We process data where authorized or needed to comply with laws (for example, tax and accounting, record-keeping, responding to lawful requests) and to enforce our terms or establish, exercise, or defend legal claims.

Artificial Intelligence Experiences: From time to time, we offer AI-powered features (for example, chatbots). Unless it's obvious from context, we will make it clear when you are interacting with an AI system rather than a human. When you use these features, you may submit text, prompts, images, or files ("Prompts"), which generate responses based on your Prompts ("Outputs"). We process your Prompts and related interaction data to generate Outputs and to operate, secure, and troubleshoot the feature.

For safety, reliability, and abuse prevention, we log technical and usage data associated with AI features (e.g., timestamps, error/abuse signals, and performance diagnostics). In limited cases, and under confidentiality obligations, authorized personnel may review a sample of minimized or de-identified prompts/outputs to investigate abuse, resolve incidents, or improve reliability. Many AI features do not require personal data; if you include personal data in a prompt, it may appear in the output you receive.

We retain AI prompts/outputs and related logs for the period necessary to operate and secure the feature and as set out in our Data Retention Policy. Where feasible, you may request deletion of prompts/outputs associated with your account; we may retain minimal suppression or audit records to honor your choices and protect the Service.

Many AI features do not require you to include personal data; if you choose to include personal data, it may appear in the Outputs. We may de-identify Prompts and Outputs and retain the de-identified data for analytics, safety, and monitoring in support of operating, securing, and fixing the feature.

We may share personal data with our AI service providers to deliver these features, under contracts that require them to act on our instructions and protect your data.

How Long Do We Keep Your Data For?

We will retain your personal data for the duration necessary for the purpose of its processing, including the provision of AI-related services and/or to meet any applicable legal obligations. Please see our Data Retention Policy, accessible at [BNI® Retention – BNI® Terms of Service](#) or more information.

How Do We Protect Your Data

We take reasonable and appropriate technical and organizational measures to safeguard your personal data against any breach, unauthorized or illegal access, alteration, disclosure, or deletion. This measure may include identity verification, encryption, access control, malicious code resistance, and regular security audits.

Our service providers (as mentioned in this Policy) may store your personal data on our behalf. We may also hold your personal data ourselves, for instance, on servers or in physical files located on our premises.

How We Disclose Your Data

We share personal data only as described below and only for the purposes set out in this Policy including as needed to provide and improve our services. Where the applicable law requires it (for example, partner marketing, nonessential cookies/SDKs, sensitive/special-category data, or cross-border transfers under PIPL), we obtain your consent first. All recipients must implement appropriate technical and organizational measures consistent with this Policy and applicable law. This does not limit our own obligations to you.

- **Service providers (processors).** We use trusted vendors to operate the service— payment processing, hosting, security/fraud prevention, analytics/measurement, email/SMS delivery, customer support tools, and AI platform providers that power optional AI features. These providers act on our instructions, must protect your data, and may not use it for their own purposes. For payments we receive tokens/confirmations and receipts from our processor; we do not store full card numbers. For AI features, providers (and their subprocessors) process your inputs (e.g., text, prompts, files) and interaction data so the feature works; we do not allow training or enrichment of AI models with your personal data unless you give explicit (GDPR) / separate (PIPL) consent for that specific use. A current list of core subprocessors is available on request.

- **Affiliates and franchisees.** To run our network and deliver the services you request, we may share business contact details and relevant account or participation information with our affiliates and franchise organizations for chapter administration, event management, member directories, and similar operational needs. Depending on the activity, these entities may act as our processors or as independent controllers under their own privacy policies. Where we operate as joint controllers for a defined activity, we will make the essence of our joint-controller arrangement available on request.

- **Members and community visibility.** If you participate in member directories, BNI Connect, chapters, referrals, or community features, as a member, guest or otherwise, your profile information (for example, name, company, role, and business contact details) and certain participation metrics may be visible to other members or chapters as part of the service. You can manage what you share in your settings where available.

- **Business partners and strategic alliances.** We share limited personal data with business partners only as described below and only for the purposes stated:

- Franchise partner organizations (Partner Program). If you join BNI through a franchisee of a participating Partner Program organization, we may share your name and membership status with that organization to verify and administer your participation in that program. We do not share your contact details with franchisors for their independent marketing purposes without your consent, where required by applicable law.
- Group Purchasing Organizations (GPOs). We may offer purchasing programs and member benefits through GPO partners. If you elect to participate in a GPO benefit, we share only the information necessary to facilitate that specific benefit with the relevant GPO partner. We do not share your contact details with GPO partners for their independent marketing purposes without your consent, where required by applicable law.
- Co-sponsored programs and affinity partners. For co-branded events, promotions, contests, webinars, or other joint programs that you choose to join, we share only the information necessary to administer the program. We do not share your contact details

with our partners for their independent marketing purposes without your consent, where required by applicable law.

- **Compliance, safety, and enforcement.** We disclose information when we must comply with law (for example, court orders, lawful requests from authorities), enforce our terms (including our Acceptable Use Policy), prevent fraud or abuse, protect our rights, users, or the public, or otherwise where we are authorized or required to do so by law.
- **Corporate transactions.** If we are involved in a merger, acquisition, reorganization, or asset sale, your information may be transferred to the successor; we will require the recipient to honor this Policy.

What Are Your Rights?

Where we process your personal data, you may have rights under applicable laws over how the data is processed. We have provided an overview of these rights below. You can exercise your rights by emailing us at [*].

- **The right to be informed.** You may have the right to be provided with clear, transparent, and easily understandable information about how we use your personal data and your rights. Therefore, we're providing you with the information in this Policy.
- **The right to withdraw consent.** Where we rely on consent, you can withdraw it at any time; this will not affect processing already carried out.
- **The right to access and rectification.** You may have the right to request access, correct, or update your personal data at any time. We understand the importance of this, and should you want to exercise your rights, please email us at compliance@bni.com.
- **The right to data portability.** The personal data you have provided us with is portable. This means it can be moved, copied, or transmitted electronically under certain circumstances.
- **The right to be forgotten.** Under certain circumstances, you may have the right to request that we delete your data. If you wish to delete the personal data we hold about you, please let us know and we will take reasonable steps to respond to your request in accordance with legal requirements. If the personal data we collect is no longer needed for any purposes and we are not required by law to retain it, we will do what we can to delete, destroy, or permanently de-identify it.
- **The right to restrict processing.** Under certain circumstances, you may have the right to restrict the processing of your personal data.
- **The right to object.** Under certain circumstances, you may have the right to object to certain types of processing, including processing for direct marketing (i.e., receiving emails from us notifying you or being contacted with varying potential opportunities).
Rights related to automated decision-making. Where available under applicable laws, you may have the right not to be subject to a decision which is based solely on automated processing and which produces legal or other significant effects on you. In particular, you may have the right: to obtain human intervention, express your point of view, and contest the decision.

If you are resident of New Zealand: To the extent applicable to you, under the Privacy Act 2020, you have the you have rights of access to and correction of your personal information in accordance with that Act. If you wish to access or update your information, please email: info@bni.co.nz. There are some circumstances under the Privacy Act 2020 when we are not obliged to provide access to the personal information we hold. If one of these situations applies to your request, we will let you know and make note of your request for access or changes that may not be completed against the relevant information.

If you have an online account with us, you can review and update your personal information online by logging into your account. You can also review and update your personal information and exercise your other rights by contacting us. More information about how to contact us is provided below. You can close your account at any time by emailing us at legal@bni.com. If you close your account, we may still retain certain information associated with your account for analytical purposes and record-keeping requirements per our Data Retention section above, as well as to prevent fraud, collect any fees owed, enforce our Terms of Service, or take other actions otherwise permitted or required by law. In addition, if certain information has already been provided to third parties as described in this Privacy Policy, retention of that information will be subject to those third parties' policies.

Third-Party Websites

Our Sites, apps, and communications may include links to, or integrations with, websites, apps, or services that are not owned or controlled by us (for example, an advertisement, a search result, an embedded video/map, social media features such as the Facebook, LinkedIn and YouTube widgets, social-sharing buttons, single-sign-on, or a checkout hosted by a payment provider). If you follow those links or interact with those features, your personal data may be collected by the third party and processed under that party's own privacy policy, not this one. These features may collect your IP address, which pages you visit our sites, and how long for. If you're a member of a social media site, the interfaces may allow the social media site to connect your visits to this site with other personal data. Social media features and midgets are either hosted by a third party or hosted directly on our Sites.

As part of this, we may provide an application programming interface ("**API**") to enable third party applications to interface with our Sites. Some applications enable you to interact with us through the API in a way that requires you to log in. To do this most of these applications will direct you through a process where you are able to let the application connect to your account. If you allow an application to connect to your account on our websites, including if you set up your account on our websites using an API with a third party social media platform, that application will be able to access information that you can see when you are logged into our websites. You should only allow applications you trust to access your account on our Sites. If you set up your account on our Sites using an API with a third party social media platform, you also consent to us obtaining and using your personal data from such platform.

Except where a third party acts as our service provider (processor) under contract (see "How we share personal data" and our Vendor & SDK Register), those third parties typically act as independent controllers of any data you provide to them. We do not endorse, control, or take responsibility for their content, security, or privacy practices, and to the maximum extent permitted by law, we accept no responsibility for the actions or omissions of those third parties.

Before you use any third-party website or feature, review its privacy and cookie notices and settings, including any choices about advertising, analytics, and tracking.

Communities and Forums Offered on our Sites

Some areas of our Sites allow you to post information about yourself (e.g., your name and email address), communicate with others, upload content, and post comments. These postings are governed by our Terms of Service. Any personal data you disclose in these areas may be visible to others with access to your content and may be collected and used by them. Please exercise discretion and caution. Once posted, you may not be able to edit or delete the data.

Children's Privacy

Our Site is designed and intended for use by adults. We do not knowingly collect personal data from children under the age applicable in your jurisdiction (for example, under 16 in the EEA; under 14 in China). If we discover that we have collected personal data from a child without consent from a parent or guardian where such consent should have been obtained under applicable laws, we will delete that personal data as soon as practical.

Data Privacy Framework

BNI Global, LLC complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. BNI Global, LLC has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. BNI Global, LLC has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>. BNI's U.S. subsidiaries adhering to the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF are: BNI Connect Global, LLC, BNI Franchising, LLC, BNI Global, LLC, BNI Global Holdings LLC, BNI Holdings, LLC, BNI Intermediate Holdings, LLC, BNI International Holdings CTB, LLC, Corporate Connections Franchising, LLC, Corporate Connections Global, LLC, Prosperity Brands, LLC, and Scion Social Holdings LLC.

Under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, you have the following rights:

- Right to choose (opt out) whether your personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you, through clear, conspicuous, and readily available mechanisms to exercise choice.
- Right to access personal information about you that we hold and the right to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of

providing access to you would be disproportionate to the risks to your privacy in the case in question, or where the rights of persons other than you would be violated.

Additional information on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF can be viewed at <https://www.dataprivacyframework.gov/s/> . The Federal Trade Commission (FTC) has jurisdiction over BNI's compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. BNI will annually renew its EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF self-certification to help ensure the treatment of all personal data continues to be accurate and processed in accordance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF principles. In cases of onward transfer to third parties of EU, UK, and Swiss Personal Data received pursuant to the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and Swiss-US DPF, BNI is potentially liable. All questions or complaints regarding the processing and use of personal data should be directed to legal@bni.com. You may also contact BNI's Data Protection Officer by email at dpo@bni.com.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, BNI Global, LLC commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit <https://www.jamsadr.com/dpf-dispute-resolution> for more information or to file a complaint. The services of JAMS are provided at no cost to you.

You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps: prior to initiating an arbitration claim: (1) raised the claimed violation directly with BNI and afforded us the opportunity to resolve the issue within the timeframe set forth in section (d)(i) of the Supplemental Principle on Dispute Resolution and Enforcement; (2) made use of the independent recourse mechanism under the Principles, at no cost to you; and (3) raised the issue through your Data Protection Authority (DPA) to the US Department of Commerce and afforded the US Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the Department's International Trade Administration, at no cost to you.

How to Contact Us

If you have any questions or concerns about BNI's Privacy Policy or data processing or if you would like to make a complaint about a possible breach of local privacy laws, please do so by contacting us by email, telephone, or mail as follows:

BNI New Zealand

Mailing Address:

16 Brisbane Street
Sydenham
Christchurch, 8023

Physical Address:

16 Brisbane Street
Sydenham
Christchurch, 8023

Phone: 09 817 1185

Email: legal@bni.com

BNI's Data Protection Officer can be contacted by email at dpo@bni.com.

Changes to this Policy

We will update this Privacy Policy when necessary to reflect customer feedback and changes in our products and services. When we post changes to this statement, we will revise the "last updated" date at the top of this Policy. We recommend that you check our Sites from time to time to inform yourself of any changes in this Policy.