Effective/Last Updated: November 15, 2025

BNI® DATA PROTECTION AND PRIVACY POLICY

BNI Worldwide Development Ltd ("BNI", "we", "our") is the controller of your personal data. In some cases, BNI Global, LLC or other BNI affiliates (collectively, "**BNI**", "**our**" or "**we**"). act as independent or joint controllers; where applicable, we will identify the relevant controller at the point of collection.

This Data Protection and Privacy Policy ("**Policy**") is intended to explain to you, as a user of BNI, our services, BNIConnect.com, or web-accessed or mobile applications ("Sites"), what personal data we collect about you, how we use or process that data, with whom it may be shared, and your options about such uses and disclosures.

If you are a California resident, please see our California Notice at Collection and Privacy Policy accessible at https://bnitos.com/ca-nacapp.

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 when you use our services, depending on your interactions with us:

- **Identification & Contact Data** such as your name, username, business or home address, email address, phone number, and account credentials used to create or manage an account.
- **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) and solely for the purpose disclosed at the time.

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 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, or contact 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)**. 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 non-essential cookies in our banner or your browser; some features may not function without them.
- **From other people and trusted partners**. A colleague or member may share your business contact details to invite you to an event or make a referral; the person sharing should have a lawful basis and, where required, 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 or assessing eligibility for a financing option), we may obtain limited credit-reference information.
- **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.

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 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, we rely on your **consent**, our **contract** with you, or our **legitimate interests**. Where the law

requires consent (for example, 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: With your permission we may: remember your settings and measure use through non-essential cookies/SDKs; send newsletters or product updates; allow partners to contact you directly about their offerings; 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. We do 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, 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 the service you requested, we create and manage your account, authenticate logins, provide core features (including AI-powered features you choose to use), process orders and subscriptions, and offer 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—for example, receipts, account or security notices, feature changes, or policy updates—so you can use the product you purchased.

Processing based on our legitimate interests: We also process personal data to keep the service secure and useful in ways that do not override your rights. This includes protecting accounts and our platform (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 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 do not make decisions based solely on automated processing that produce legal or similarly significant effects about you without human involvement. If that ever changes, we will provide specific notice and explain your rights, including the ability to obtain human review, express your view, and contest the decision.

We may share personal data with our AI service providers solely 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 https://bnitos.com/retention.html for 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.

How We Disclose Your Data

We share personal data only as described below and only for the purposes needed to provide and improve our services. Where the law requires it (for example, partner marketing, non-essential 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 choose to participate in member directories, chapters, referrals, or community features, the profile information you provide (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** (co-sponsored offerings). For co-branded events, promotions, contests, or webinars that you choose to join, we share only the information necessary to run the program and, where required by law, we obtain your opt-in before a partner may market to you directly. You can opt out at any time.
- **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, or protect our rights, users, or the public.
- **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.

Cross-Border Transfers

This section covers transfers to our affiliates/franchisees, members, business partners, and service providers when they are located outside your country. When your personal data is transferred outside your country, we apply safeguards designed to ensure a level of protection essentially equivalent to that required by applicable law.

EEA/UK/Switzerland. If you are located in the EEA, the UK, or Switzerland, we rely on:

- Adequacy decisions where available (EU/UK/CH).
- Standardized transfer tools where adequacy is not available, including the EU Standard Contractual Clauses (SCCs), the UK IDTA/Addendum, and the Swiss FDPIC addendum, as applicable.
- Transfer impact assessments and supplementary measures (for example, encryption in transit and at rest, strict access controls, minimization/pseudonymization, and contractual limits on onward disclosure).

If you are a resident of China, we will obtain separate consent before we share, transfer, or store (export) personal data. The name and contact details of overseas recipients, the purpose and method of processing, the categories of personal information exported, the retention period, and our transfer mechanism are set out in our Vendor & SDK Register below. We use an approved export path (e.g., CAC security assessment, certification, or the China

Standard Contract filing) as legally required. You may withdraw consent at any time; doing so may limit features that rely on the export.

Onward transfers to vendors/sub-processors. Any overseas service providers that process personal data on our behalf must act on our instructions, implement appropriate security measures, and agree to equivalent protections for any onward disclosures.

Vendor & SDK Register

We maintain the following third-party tools. This list reflects the current core set and may change; when it does, we will update this register and, where required, notify you or seek consent again.

Provider	Schoox
Role	Processor
Purpose of Use	Member Training
Personal Data Processed	Member name, member email address
Processing Locations	United States, United Kingdom, Canada
Cross-Border Mechanisms	• EU-U.S. Data Privacy Framework (EU-U.S. DPF) Principles for personal data received from the European Union and Gibraltar. • UK Extension to the EU-U.S. Data Privacy Framework (UK Extension to the EU-U.S. DPF) Principles for personal data received from the United Kingdom. • Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) Principles for personal data received from Switzerland.
Retention / Deletion	Schoox commits to the following in their published privacy policy, "**Storage limitation** – Data is kept only for as long as necessary for the purposes we have communicated."
Privacy Policy	https://www.schoox.com/privacy.php

Provider	Marketo
Role	Processor
Purpose of Use	Member marketing communication and management
Personal Data Processed	Member name, member email address, phone number, business address, member gender (optional)
Processing Locations	The Marketo Engage service infrastructure is located in data centers in the United States, the United Kingdom, the Netherlands, and Australia.
Cross-Border Mechanisms	Adobe uses several legal mechanisms, including Standard Contractual Clauses (SCCs) and adequacy decisions (where applicable).
Retention / Deletion	Marketo has a defined retention policy for lead activities up to 25 months
Privacy Policy	https://www.adobe.com/privacy/policy.html

Provider	Creatio
Role	Processor
Purpose of Use	Customer relationship management system

Personal Data Processed	Member name, member email address, phone number, business address, member gender (optional)
Processing Locations	Creatio's cloud application is hosted on **Amazon Web Services (AWS)** and **Microsoft Azure**. Customers can choose from data centers located around the world.
Cross-Border Mechanisms	Data may be transferred and processed outside the EU/EEA. Creatio states it "may use **standard data protection clauses** adopted by supervisory authorities and approved by the European Commission" to safeguard these transfers.
Retention / Deletion	**Closed Profiles:** Deleted within 15 business days of a request. **Backups:** Kept for 90 calendar days. **Billing & Legal Info:** Kept for 10 years. **Process Logs:** Automatically deleted or archived after 30 days.
Privacy Policy	https://www.creatio.com/privacy-policy

Provider	KCADI, LTD
Role	Processor
Purpose of Use	Data analysis and reporting
Personal Data Processed	Name, email, phone number, business and billing address, business name, member gender (optional)
Processing Locations	United Kingdom
Cross-Border Mechanisms	N/A
Retention / Deletion	N/A
Privacy Policy	N/A

What Are Your Rights?

Where we process your personal data, you have a number of rights over how the data is processed and can exercise these rights at any point. We have provided an overview of these rights below. You can exercise your rights by emailing us at [*].

- **The right to be informed.** You 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 have the right to 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 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 have the right to restrict the processing of your personal data.
- **The right to object**. Under certain circumstances, you 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).
- You have the right to complain to a data protection authority about our collection and use of your personal information. You may lodge a complaint with a supervisory authority where you live or work, or where the alleged infringement occurred. Contact details for **data protection authorities in the EEA here**, in the UK **here**, and in Switzerland **here**.
- Rights related to automated decision-making. You 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 have the right: to obtain human intervention, express your point of view, and contest the decisio.

If you are a resident of China under the Personal Information Protection Law of the People's Republic of China (PIPL), you have the following rights:

- Right to access and copy of data.
- Right to transfer.
- Right to correct or supplement.
- Right to deletion in certain circumstances.
- Right to limit or withdraw consent.
- Right to request details of processing (including for automated decision-making, and can refuse such decision) and of handling rules.
- Right to deregister accounts.
- Right to make a complaint to the Cybersecurity Administration of China (CAC).

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 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-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 directly by the third party and processed under that party's own privacy policy, not this one.

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. 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 voluntarily 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, 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 Worldwide Development Ltd
Ballinrobe Road
Castlebar
Co. Mayo
F23 FT28
IRELAND
Phone: +353 94 902 1553
Email: legal@bni.com

BNI's Data Protection Officer can be contacted at the above address or phone number, or by email at dpo@bni.com.

If you are a resident of China, please contact us at:

Regus Tianhe Teem Tower Centre
27/F Teem Tower
208 Tian He Road
Tian He District
Guangzhou, 510620
P.R. China
Phone: 86-020-28261855
Email: info.china@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. We will not reduce your rights under this Policy without your consent.