

NETLY PRIVACY POLICY

Protection of Personal Information — Complete Policy Document

Effective date: April 1, 2026
Last revised: September, 15, 2026

Vision Concurrence Inc., operating as NETLY
Québec, Canada | support@netly.ca | netly.ca/confidentialite

NETLY's commitment: we only collect what is necessary. We use your information solely for the purposes disclosed. We never sell your personal information. We protect your rights under Law 25 and PIPEDA. This document is written to be understood, not to obscure.

ARTICLE 1 — IDENTITY OF THE ORGANIZATION RESPONSIBLE FOR PERSONAL INFORMATION

Who is responsible for your personal information

The organization responsible for the collection, use, disclosure, and retention of personal information within the NETLY platform is:

Field	Details
Legal name	Vision Concurrence Inc.
Trade name	NETLY
Province of incorporation	Québec, Canada
Primary market	Province of Québec, Canada
Platform	NETLY mobile application (iOS and Android) and website netly.ca
Privacy Officer	Designated officer — contact: confidentialite@netly.ca
General inquiries	support@netly.ca

The Privacy Officer designated by Vision Concurrence Inc. is responsible for ensuring compliance with this Privacy Policy and applicable personal information protection legislation, processing requests to exercise rights, and overseeing all of NETLY's personal information protection practices.

ARTICLE 2 — SCOPE AND APPLICABLE LEGISLATION

Who this policy applies to and which laws govern it

2.1 Scope

This Privacy Policy applies to all individuals whose personal information is collected, used, disclosed, or retained by NETLY in connection with the Platform, including:

- Clients — individuals who use the NETLY Platform to book home and personal care services;
- Service Providers — individuals and businesses registered on NETLY to offer and perform services;
- Website visitors — individuals who browse netly.ca without creating an account;
- Prospective candidates and partners who submit personal information to NETLY;
- Advertisers — Service Providers or external businesses who post a Sponsored Listing on the Platform, whether or not they hold a NETLY user profile.

2.2 Applicable legislation

NETLY's personal information practices are governed by the following laws, in order of priority in the event of conflict:

Legislation	Jurisdiction and key requirement
-------------	----------------------------------

Act Respecting the Protection of Personal Information in the Private Sector, as amended by Law 25	Québec — primary applicable law; sets the highest standards for consent, incident notification, privacy impact assessments (PIAs), and individual rights, including the right to de-indexing
Personal Information Protection and Electronic Documents Act (PIPEDA)	Federal, Canada — baseline standard for private-sector organizations operating across provinces
Canada’s Anti-Spam Legislation (CASL)	Federal, Canada — governs all commercial electronic messages sent by NETLY
Consumer Protection Act (Québec)	Québec — applies to NETLY’s commercial relationships with consumers
Any other applicable provincial privacy legislation	Applicable depending on the User’s province of residence

Where Québec’s Law 25 applies — which is the case for the vast majority of NETLY users — it imposes stricter obligations than PIPEDA, including: mandatory privacy impact assessments before implementing new technologies involving personal information, notification to the Commission d’accès à l’information (CAI) and affected individuals as soon as possible in the event of a privacy incident presenting a risk of serious harm, and enhanced individual rights.

In all circumstances, NETLY applies the most protective standard available under applicable legislation.

2.3 Amendments to this policy

NETLY reserves the right to amend this Privacy Policy at any time. The revised policy will be posted on the Platform with an updated “Last Revised” date. For material amendments — as determined by NETLY in good faith — we will notify Users through the application or by email at least 30 days before the change takes effect. Your continued use of the Platform after that date constitutes acceptance of the revised policy.

ARTICLE 3 — DEFINITIONS

Key terms used throughout this policy

The following definitions apply throughout this Privacy Policy:

Term	Definition
Personal information	Any information that directly or indirectly relates to an identified or identifiable natural person. This includes names, contact details, identification numbers, location data, and any other information that could, alone or combined with other data, identify a person.
Sensitive personal information	A subset of personal information requiring enhanced protection due to the particular risk of harm associated with its unauthorized use or disclosure, including financial data, government identification numbers, health information, biometric data, criminal background check reports, and information concerning minors.
Processing	Any operation performed on personal information, including collection, recording, organization, retention, use, disclosure, transfer, anonymization, and destruction.
Client	A NETLY User who books and pays for services through the Platform.
Service Provider / Pro	A NETLY User registered to offer and perform services through the Platform.
Platform	The NETLY mobile application (iOS and Android) and the website netly.ca.
PSP	Payment Service Provider — the third-party processor (e.g., Stripe) that processes all financial transactions on the Platform, including the temporary escrow of Client payments and payouts to Service Providers.
KYC	Know Your Customer — the verification process carried out before a User can access certain Platform features, including, for certain categories of Service Providers, a vulnerable sector criminal background check.
Privacy Officer	The person designated by Vision Concurrence Inc. to oversee compliance with applicable privacy legislation and this Policy.
Privacy incident	Any unauthorized access, collection, use, disclosure, or loss of personal information likely to cause harm to the individuals concerned.
Consent	A free, informed, and unambiguous expression of will by which a person agrees to the processing of their personal information for specified purposes.
Anonymization	An irreversible process of modifying personal information so that the individual can no longer be identified, directly or indirectly, even by NETLY.

ARTICLE 4 — CONSENT — THE BASIS OF ALL PROCESSING

How we obtain and manage your consent

4.1 Principle of consent

NETLY does not collect, use, or disclose personal information without a valid legal basis. In most cases, this basis is your freely given, informed, and specific consent. In certain cases, processing may be necessary to perform a contract with you, to comply with a legal obligation, or to serve a legitimate interest that does not override your fundamental rights.

4.2 How consent is obtained

NETLY obtains consent through the following mechanisms:

- Account creation — when creating a NETLY account, this Privacy Policy and our Terms of Use are presented to you. Proceeding with registration constitutes your informed consent to the processing of your personal information as described herein;
- Specific consent for criminal background check purposes — by agreeing to use the Platform and to provide the required identity documents, the Service Provider consents to NETLY, or its verification partner, conducting a criminal background check where required under the Terms of Use, notably for service categories involving direct contact with minors or a vulnerable clientele;
- Granular in-app consent — for specific processing activities requiring separate consent (marketing communications, optional tracking technologies), we obtain explicit consent through clearly presented prompts within the Platform;
- Implied consent — where processing is directly related to a transaction you have initiated and the purpose is evident, consent may be inferred from the context.

4.3 Withdrawal of consent

You have the right to withdraw your consent at any time for purposes based on consent. Withdrawal of consent does not affect the lawfulness of processing carried out before such withdrawal. To withdraw your consent, contact us at confidentialite@netly.ca or use the account settings within the Platform.

Where withdrawal of consent prevents NETLY from fulfilling its contractual obligations to you (for example, processing a Booking, or maintaining a Service Provider's registration in a service category subject to mandatory verification), we will inform you before acting on the withdrawal.

4.4 Consent of minors

NETLY does not knowingly collect personal information from individuals under the age of 18. If we become aware that a minor has submitted personal information without appropriate parental consent, we will delete that information without delay and deactivate the account concerned. Parents or guardians who believe a minor has registered on NETLY should contact us immediately at confidentialite@netly.ca.

ARTICLE 5 — PERSONAL INFORMATION WE COLLECT

A complete inventory of what we collect and how

5.1 Information you provide directly

Category	Examples	Source
Identity information	Full legal name, date of birth	Account registration; KYC process
Government-issued ID	Driver's licence number, passport number (type only — not retained in raw form)	KYC verification — transmitted solely to the verification partner
Contact details	Email address, phone number, home or service address	Account registration; Booking process
Authentication credentials	Username, salted and hashed password	Account creation
Profile content	Profile photo, service descriptions, biography (Service Providers)	User-generated content; voluntarily uploaded
Professional documentation	Business registration number (NEQ), licence or permit numbers, general liability insurance certificate details	Service Provider onboarding — in accordance with Sections

		4.2, 4.2.1, and 4.2.2 of the Terms of Use
Criminal background check	Verification result (pass, fail, or flag); for Service Providers offering childcare, elder care, or any other service involving direct, unsupervised contact with a vulnerable clientele, this report is mandatory, dated less than 6 months prior, includes a vulnerable sector check, and must be renewed every 12 months	Provided by the Service Provider, ordered by NETLY at their request, or transmitted by the verification partner — in accordance with Section 4.2 of the Terms of Use
Booking data	Service type requested, date, time, service address, special instructions	Booking creation by the Client
Payment history (Clients)	Transaction history, refunds issued, downloadable invoices and receipts	Automatically generated by Platform operations; refunds processed directly by the PSP to the original payment method
Earnings and payouts (Providers)	Payout and balance history — accessed directly via the Service Provider's Stripe Express Dashboard; NETLY does not collect or retain this data itself	Generated and retained by the PSP; NETLY receives only payout confirmation
In-app communications	Messages exchanged between the Client and the Service Provider via the Platform's messaging feature	In-app messaging feature
Reviews and ratings	Written reviews and numerical ratings submitted after a completed Booking	Post-service review process
Customer service communications	Emails, in-app messages, or calls to the NETLY support team	Contact initiated by the user with NETLY
Financial information (indirect)	Banking details are collected and processed by our PSP. NETLY does not retain raw card data.	The PSP processes payment; NETLY receives only the status and confirmation of the transaction
Feedback and survey responses	Responses to optional in-app surveys	Voluntary user submission
Advertiser information (Sponsored Listings)	Business name, logo, description, website, phone number, address, contact name	Provided by the Service Provider when requesting a Listing, or entered by NETLY administration for an external Advertiser

Note: In accordance with Section 4.2 of the Terms of Use, NETLY does not systematically collect proof of CNESST (Québec's workplace safety board) standing from Service Provider businesses employing personnel. Such proof may be requested on a case-by-case basis, at NETLY's discretion, as part of a spot check or a dispute — it does not form part of the personal information retained in a Service Provider's ongoing file.

5.2 Information collected automatically

When you use the NETLY Platform, we automatically collect the following technical data:

- Device identifiers — device type, operating system version, unique device identifier;
- Network information — IP address, mobile network carrier;
- Approximate geolocation — city/region level, derived from IP address, used to display service availability. We do not collect precise GPS coordinates without your explicit consent;
- Usage data — features accessed, screens visited, session duration, navigation patterns, errors encountered;
- Crash and performance logs — anonymized diagnostic data used to identify and fix technical issues;
- Authentication tokens — session tokens used to securely maintain your logged-in state;
- Interactions with Sponsored Listings — views, clicks, and contact interactions, tracked in aggregate and communicated to the relevant Advertiser for performance-tracking purposes.

Note: We do not collect real-time GPS geolocation data. Geolocation is approximate and used solely to match Users with available service areas.

5.3 Information received from third parties

In limited circumstances, we receive information about you from external sources:

- Payment Service Provider (PSP): transaction status, payment confirmation, and fraud signals — used to process Bookings and protect against financial fraud;
- Identity verification partners: the result of the KYC verification (pass, fail, or flag) and, where applicable, the result of the criminal background check — not the underlying document images, which are processed by the verification partner under its own confidentiality obligations;
- App distribution platforms: the Apple App Store and Google Play may share aggregated download statistics. They do not share individual user data with NETLY without your consent;
- Publicly available sources: where relevant for fraud prevention or Service Provider background checks (e.g., public business registry data, Québec’s enterprise registrar).

NETLY does not purchase personal information from data brokers, commercial data aggregators, or advertising platforms.

5.4 Information we do not collect

NETLY expressly does not collect:

- Raw payment card numbers, CVVs, or bank account credentials (processed exclusively by the PSP);
- Biometric data (facial recognition, fingerprints) beyond what is processed by identity verification partners during KYC;
- Health or medical information;
- Information concerning individuals under the age of 18;
- Racial or ethnic origin, political opinions, religious beliefs, sexual orientation, or union membership, except where voluntarily disclosed by the User within their profile content.

ARTICLE 6 — PURPOSES FOR PROCESSING PERSONAL INFORMATION

Why we process your information — purpose by purpose

NETLY processes personal information only for specific, explicit, and legitimate purposes. The table below maps each purpose to its legal basis under applicable legislation.

Purpose	Information used	Legal basis
Creating and managing your NETLY account	Identity, contact details, credentials	Contract performance
Processing Bookings and payments	Booking data, identity, transaction status	Contract performance
KYC identity verification	Government ID, proof of address, selfie	Legal obligation + legitimate interest (Platform integrity)
Mandatory criminal background check for vulnerable-clientele service categories (childcare, elder care)	Criminal background check report, including vulnerable sector check	Legal obligation + overriding legitimate interest (protection of vulnerable persons) + Service Provider’s explicit consent
Sending transactional communications (confirmations, receipts, reminders, service updates)	Contact details, Booking data	Contract performance
Customer service and dispute resolution	Communications, Booking data, in-app messages, reviews	Legitimate interest + contract performance
Fraud detection and prevention	Device data, IP address, usage patterns, transaction data	Legitimate interest + legal obligation
Platform security and infrastructure integrity	Technical logs, authentication tokens, device identifiers	Legitimate interest
Platform improvement (analytics, bug fixes, feature development)	Anonymized or aggregated usage data	Legitimate interest
Displaying regional service availability	Approximate geolocation (IP-based)	Contract performance + legitimate interest
Marketing communications about NETLY features, promotions, or new service categories	Contact details, usage preferences	Explicit consent (opt-in only — CASL-compliant)

Compliance with legal and regulatory obligations (tax records, law enforcement requests, court orders)	As required by the competent authority	Legal obligation
Evaluation or execution of business transactions (merger, acquisition, asset sale)	User data as business assets	Legitimate interest (with prior notice to Users)
Managing Sponsored Listings and measuring performance	Advertiser information, view/click/interaction statistics	Contract performance + legitimate interest
Processing refunds to Clients and payouts to Service Providers	Transaction data, payment method, Service Provider's individual Stripe account	Contract performance

NETLY DOES NOT SELL, RENT, ASSIGN, OR TRANSFER YOUR PERSONAL INFORMATION TO THIRD PARTIES FOR ADVERTISING OR COMMERCIAL PURPOSES. YOUR DATA IS USED EXCLUSIVELY TO OPERATE THE NETLY PLATFORM AND FOR THE PURPOSES DISCLOSED IN THIS POLICY. THIS PROHIBITION IS ABSOLUTE AND WITHOUT EXCEPTION.

ARTICLE 7 — DISCLOSURE OF PERSONAL INFORMATION

Who receives your personal information and under what conditions

7.1 Disclosure between Users

To function as a matchmaking Platform, NETLY makes certain information visible between Users:

- Clients may view a Service Provider's public profile: display name, profile photo, service categories, ratings and reviews;
- When a Booking is confirmed, the Service Provider receives the Client's first name, service address, and service description;
- Messages exchanged in-app between a Client and a Service Provider are accessible to NETLY's support team for dispute resolution purposes, as disclosed at the time of Booking;
- Reviews submitted by Clients are published on the Service Provider's profile.

NETLY does not disclose: *a Client's full legal name, phone number, or email address to a Service Provider, or vice versa, except with the User's explicit authorization.*

7.2 Disclosure to service partners (processors)

NETLY relies on a limited number of carefully selected third-party service providers who process personal information on NETLY's behalf and under its instructions:

Partner category	Purpose	Information disclosed
Payment Service Provider (e.g., Stripe)	Processing all financial transactions; temporary escrow of Client payments; individual payouts to Service Providers' Stripe Express accounts; fraud detection	Client banking details; transaction amounts; Service Provider banking and identity information — processed directly by the PSP under its own KYC process; NETLY receives only transaction and payout status
Identity and background check verification partner	KYC verification of Users prior to first Booking or payment; criminal background checks (including vulnerable sector checks) for relevant service categories	Government ID images; proof of address; selfie; background check request — transmitted for verification; result communicated to NETLY; documents not retained by NETLY
Cloud infrastructure provider / host	Secure storage and processing of Platform data	All Platform data, retained under strict contractual data protection obligations
Analytics provider (anonymized)	Understanding Platform usage to improve features and fix bugs	Anonymized or aggregated usage data only — no personal identifiers transmitted
Customer service platform	Managing and resolving User support requests	Support communications, account identifiers — subject to a data processing agreement
Email delivery provider	Sending transactional and marketing communications	Email address, name, communication content — subject to a data processing agreement

All service partners are bound by written data processing agreements that: (i) restrict their use of personal information to the purposes specified by NETLY; (ii) prohibit subcontracting without NETLY's prior written consent; (iii) require the implementation of appropriate technical and organizational security measures; and (iv) require prompt notification to NETLY in the event of a security incident.

7.3 Disclosure required by law

NETLY may disclose personal information without your consent where legally required to do so under a court order, subpoena, warrant, or other legally enforceable request from a competent authority. In such cases, NETLY will:

- Disclose only the minimum information required to comply with the legal request;
- Notify the affected User of the disclosure as soon as legally permitted;
- Where legally available, challenge or seek to narrow overly broad requests for personal information;
- Maintain a record of all such disclosures and make summary information available in its annual transparency report.

7.4 Disclosure in connection with a business transaction

In the event Vision Concurrence Inc. undergoes a merger, acquisition, reorganization, or sale of all or substantially all of its assets — in accordance with Section 21 of the Terms of Use — personal information held by NETLY may be transferred to the acquiring entity. In such circumstances, NETLY will:

- Notify Users of the impending transfer at least 30 days before it takes place;
- Ensure the receiving entity offers equivalent privacy protections and is bound by terms at least as protective as this Policy;
- Where required by Law 25, obtain renewed consent from Users for any material change in processing purpose;
- Offer Users the opportunity to delete their accounts before the transfer is finalized.

7.5 Prohibition on the sale of personal information

NETLY DOES NOT SELL, RENT, LEASE, OR TRANSFER YOUR PERSONAL INFORMATION TO THIRD PARTIES FOR MONETARY OR OTHER CONSIDERATION. THIS PROHIBITION IS ABSOLUTE AND APPLIES REGARDLESS OF THE FORM OF THE TRANSACTION OR THE IDENTITY OF THE RECIPIENT.

ARTICLE 8 — TRANSFERS OF PERSONAL INFORMATION OUTSIDE QUÉBEC AND CANADA

When your data crosses provincial or national borders

NETLY is headquartered in Québec and retains data primarily on servers located in Canada. However, certain of our service partners operate infrastructure in other jurisdictions, notably the United States. Where personal information is processed outside Québec or Canada, it may be subject to the laws of that jurisdiction.

8.1 Law 25 requirements for transfers outside Québec

Under Québec's Law 25, before disclosing personal information outside Québec, NETLY must:

1. Conduct a privacy impact assessment (PIA) to evaluate the level of protection offered by the destination jurisdiction relative to Québec standards;
2. Implement contractual protective measures — including data processing agreements — to ensure the recipient offers protections equivalent to those required under Québec law;
3. Disclose in this Privacy Policy the fact that personal information may be disclosed outside Québec, along with the destination country or territory where known;
4. Ensure that the disclosure is limited to what is strictly necessary for the intended purpose.

8.2 Known jurisdictions of cross-border processing

Personal information processed by NETLY's service partners may be transferred to or processed in the following jurisdictions:

- United States of America — primary jurisdiction for the PSP (Stripe) and certain cloud infrastructure providers;
- European Union — potential jurisdiction for certain analytics or support tools.

NETLY has conducted, or is in the process of conducting, PIAs for all cross-border transfers and has implemented appropriate contractual protective measures, including standard contractual clauses where applicable.

8.3 Your rights regarding cross-border transfers

You may request information about specific transfers of your personal information outside Québec, including the identity of the recipient and the processing jurisdiction, by contacting our Privacy Officer at confidentialite@netly.ca.

ARTICLE 9 — RETENTION OF PERSONAL INFORMATION

How long we retain your data — and why

NETLY retains personal information only for as long as necessary to fulfill the purposes for which it was collected, subject to applicable legal retention requirements and in accordance with Section 9 of the Terms of Use. Upon expiry of the applicable retention period, personal information is securely deleted or irreversibly anonymized.

Data category	Retention period	Basis
Account information (name, contact details, credentials) and transaction history	Duration of active account + 7 years after closure	Legal obligation — tax and accounting compliance (Revenu Québec / CRA); consistent with Section 9 of the Terms of Use
Booking records and transaction history	7 years from the date of the transaction	Legal obligation — tax and accounting law (Revenu Québec / CRA)
In-app communications between Users	24 months from the exchange, or until full resolution of an ongoing dispute if relevant	Legitimate interest — dispute resolution; consistent with Section 9 of the Terms of Use
KYC identity documents (ID images, proof of address)	Deleted within 30 days following verification by the verification partner. Result (pass/fail) retained for the duration of the account + 7 years.	Data minimization principle; legal obligation
Criminal background check reports (vulnerable sector)	Result retained for the duration of the Service Provider's registration in the relevant service category, renewed every 12 months; underlying report not retained beyond verification	Legal obligation + overriding legitimate interest (protection of vulnerable persons); consistent with Section 4.2 of the Terms of Use
Support tickets and customer communications	3 years from the date of resolution	Legitimate interest — quality assurance; potential legal claims
Technical and usage logs	12 months, then anonymized or deleted	Legitimate interest — security monitoring; Platform improvement
Marketing consent records	Duration of consent + 3 years after withdrawal	Legal obligation — CASL proof of consent
Fraud and security incident records	5 years from the date of the incident	Legal obligation; legitimate interest — fraud prevention
Anonymized / aggregated analytics data	Indefinitely (no personal identifiers)	No longer constitutes personal information after anonymization

When you request deletion of your account, NETLY initiates a deletion process within 30 days. Certain data may be retained beyond account closure where required by law or for the defence of legal claims. You will be informed of any such retention at the time of your request.

ARTICLE 10 — SECURITY — HOW WE PROTECT YOUR PERSONAL INFORMATION

Technical and organizational security measures

10.1 Our security framework

NETLY implements a layered, risk-based security framework designed to protect personal information against unauthorized access, disclosure, alteration, loss, or destruction. Our measures include:

Technical measures:

- Transport layer security (TLS 1.2 or higher) for all data in transit between your device and our servers;
- Encryption at rest for sensitive personal data stored on our infrastructure;
- Password hashing using bcrypt or an equivalent industry-standard cryptographic algorithm — passwords are never stored in plain text;
- Multi-factor authentication available for User accounts;
- Token-based session management with automatic expiry and invalidation upon logout;
- Payment data isolation — raw card data never reaches NETLY’s systems; all payment processing is performed by the PCI-DSS compliant PSP;
- Regular vulnerability scans and penetration testing of the Platform infrastructure;
- Automated monitoring and alerting for abnormal access patterns or security events.

Organizational measures:

- Access to personal information is limited to NETLY personnel with a documented business need, on a least-privilege basis;
- All personnel with access to personal information receive privacy and security training upon onboarding and annually thereafter;
- All service partners that process personal information on NETLY’s behalf are bound by data processing agreements requiring equivalent security standards;
- NETLY maintains an internal privacy and security policy document governing data processing practices;
- A designated Privacy Officer oversees all personal information protection activities.

NO METHOD OF INTERNET TRANSMISSION OR ELECTRONIC STORAGE IS COMPLETELY SECURE. WHILE NETLY TAKES ALL COMMERCIALLY REASONABLE MEASURES TO PROTECT YOUR PERSONAL INFORMATION, WE CANNOT GUARANTEE ABSOLUTE SECURITY. ANY TRANSMISSION OF DATA TO OR FROM THE PLATFORM IS AT YOUR OWN RISK. NETLY IS NOT RESPONSIBLE FOR THE CIRCUMVENTION OF SECURITY MEASURES BY UNAUTHORIZED THIRD PARTIES.

10.2 Privacy incident response

In the event of a privacy incident involving personal information under NETLY’s control, we will:

5. Immediately investigate the incident to determine its scope, nature, and cause;
6. Implement containment measures to prevent any further unauthorized access or disclosure;
7. Assess the risk of harm to affected individuals;
8. Notify the Commission d’accès à l’information (CAI) of Québec as soon as possible following becoming aware of an incident presenting a risk of serious harm — in accordance with Law 25;
9. Inform affected individuals as soon as possible where the incident presents a risk of serious harm, providing sufficient detail to allow them to take protective measures;
10. Maintain a register of all privacy incidents in accordance with Law 25;
11. Implement corrective measures to prevent recurrence.

ARTICLE 11 — COOKIES, TOKENS, AND TRACKING TECHNOLOGIES

What we use, why, and how to control it

NETLY uses a minimal set of tracking technologies. We do not use third-party advertising trackers, behavioral profiling tools, or persistent cross-site tracking mechanisms.

Technology	Purpose	Opt-out available
Session authentication tokens (application)	Securely maintain your logged-in session during active use. Strictly necessary.	No — required for application functionality

Session cookies (website)	Maintain your logged-in state on netly.ca. Strictly necessary.	No — required for website functionality
Crash and performance analytics (anonymized)	Detection and resolution of technical errors. No personal identifiers transmitted.	Yes — contact confidentialite@netly.ca
Optional analytics cookies (website)	Understand visitor navigation on netly.ca to improve content. Deployed only with your consent.	Yes — via the cookie consent banner on first visit
Marketing cookies (website only)	Measure the effectiveness of NETLY's marketing campaigns. Deployed only with your explicit consent.	Yes — withdraw consent at any time via account settings or cookie settings

You may manage browser cookies through your browser settings at any time. Disabling strictly necessary cookies may impair Platform functionality. Disabling optional cookies will not affect your ability to use the Platform's core features.

We do not: use pixel tags, device fingerprinting, or cross-site tracking for advertising purposes. We do not share User behavioral data with advertising networks.

ARTICLE 12 — YOUR RIGHTS UNDER APPLICABLE PRIVACY LEGISLATION

A complete statement of your privacy rights

Québec's Law 25 and PIPEDA grant you meaningful, enforceable rights over your personal information. NETLY is committed to respecting and facilitating the exercise of these rights. Below is a complete statement of your rights and how to exercise them.

Your right	What it means	How to exercise it
Right to be informed	The right to know, before or at the time of collection, what personal information is collected, for what purposes, and with whom it is shared.	This Privacy Policy is the primary vehicle for this right. Contact confidentialite@netly.ca for specific questions.
Right of access	The right to obtain confirmation that NETLY holds personal information about you and to receive a copy of it in a structured format.	Submit a written request to confidentialite@netly.ca with the subject line: Access Request.
Right of rectification	The right to have inaccurate or incomplete personal information corrected or updated.	Update directly via account settings or contact confidentialite@netly.ca.
Right to deletion (right to erasure)	The right to request deletion of your personal information when it is no longer necessary, when you withdraw consent, or when processing is unlawful — subject to legal retention requirements.	Submit a request to confidentialite@netly.ca with the subject line: Deletion Request.
Right to withdraw consent	The right to withdraw consent to consent-based processing at any time, without affecting the lawfulness of processing carried out before withdrawal.	Use in-app settings for marketing preferences or contact confidentialite@netly.ca.
Right to data portability	The right to receive your personal information in a structured, commonly used, machine-readable format, and to transmit it to another organization.	Submit a request to confidentialite@netly.ca with the subject line: Portability Request.
Right to object to automated decisions	The right to request human review of any significant decision made exclusively through automated processing that affects you.	Contact confidentialite@netly.ca immediately upon becoming aware of such a decision.
Right to de-indexing (Law 25)	The right to request that personal information published on the Platform — including reviews or profile information — be de-indexed from search engines, where its continued indexing causes harm and no legitimate public interest exists.	Submit a written request to confidentialite@netly.ca with the subject line: De-indexing Request.
Right to restrict processing	The right to request that NETLY restrict the processing of your personal information in certain circumstances (e.g., while disputing accuracy or assessing an objection).	Contact confidentialite@netly.ca with the subject line: Restriction Request.

12.1 How to submit a request to exercise your rights

To exercise any of the rights described above:

12. Send an email to confidentialite@netly.ca with a clear description of your request and a subject line identifying the right you wish to exercise;
13. Include your full name and the email address associated with your NETLY account so that we can verify your identity;
14. NETLY will acknowledge receipt within 5 business days;
15. We will respond to your request within 30 days. For complex requests, we may extend this period by an additional 30 days, with written notice and explanation;
16. We do not charge a fee for standard requests to exercise rights. For manifestly unfounded or excessive requests, we may charge a reasonable administrative fee, of which we will inform you in advance.

12.2 Identity verification

To protect against unauthorized access to your personal information, NETLY will verify your identity before processing any request to exercise rights. Verification may require confirming information associated with your account. We will not act on a request from a person we cannot reasonably verify as the account holder.

12.3 Right to file a complaint with a supervisory authority

If you believe NETLY has failed to respect your privacy rights or has otherwise failed to comply with applicable legislation, you have the right to file a complaint with the competent supervisory authority:

- Québec residents: Commission d'accès à l'information du Québec (CAI) — cai.gouv.qc.ca — 1-888-528-7741;
- All Canadian residents: Office of the Privacy Commissioner of Canada — priv.gc.ca — 1-800-282-1376.

We encourage you to first contact our Privacy Officer, as many concerns can be resolved quickly without a formal complaint process. However, your right to contact the supervisory authority directly is unconditional and is not contingent on prior contact with NETLY.

ARTICLE 13 — MARKETING COMMUNICATIONS AND CASL COMPLIANCE

Our commitment to consent-based marketing

NETLY fully complies with Canada's Anti-Spam Legislation (CASL), which requires express or implied consent before sending commercial electronic messages (CEMs). We take this obligation very seriously.

- We send marketing communications — newsletters, promotional offers, new feature announcements — only to Users who have explicitly opted in through the Platform;
- Every marketing message includes a clear, functional, and permanent unsubscribe mechanism;
- Unsubscribe requests are processed within 10 business days in accordance with CASL;
- We retain records of all marketing consents, including the date, method, and scope of consent, for at least 3 years after expiry or withdrawal of consent;
- Transactional communications — Booking confirmations, receipts, security alerts, account notifications — are not marketing messages and are sent regardless of marketing consent status.

Unsubscribe at any time: *Use the unsubscribe link in any marketing email, or manage your communication preferences in Account Settings within the application.*

ARTICLE 14 — PRIVACY IMPACT ASSESSMENTS (PIAs)

Proactive privacy protection for new technologies

Under Québec's Law 25, NETLY is required to conduct a privacy impact assessment (PIA) before implementing any technology or business process involving personal information that presents privacy risks. This obligation applies to new Platform features, new service partners, and cross-border data transfers.

A PIA is an internal risk analysis that: (i) identifies the personal information involved; (ii) maps data flows and processing activities; (iii) assesses the sensitivity of the information and potential risks; (iv) evaluates the adequacy of planned safeguards; and (v) identifies additional measures required before implementation.

PIAs are conducted by our Privacy Officer and reviewed before launching any new data processing activity. Where a PIA identifies significant risks that cannot be adequately mitigated, the project will be halted or redesigned before proceeding.

Transparency: *We publish summary information about our PIA practices in our annual privacy report. To request a copy, contact confidentialite@netly.ca.*

ARTICLE 15 — LIMITATION OF LIABILITY REGARDING PRIVACY PROTECTION

NETLY's liability framework regarding privacy

While NETLY takes all commercially reasonable measures to protect personal information and comply with applicable privacy legislation, certain limits apply to NETLY's liability in this regard, consistent with Section 13 of the Terms of Use.

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, NETLY SHALL NOT BE LIABLE FOR: (A) UNAUTHORIZED ACCESS TO PERSONAL INFORMATION RESULTING FROM SECURITY INCIDENTS BEYOND NETLY'S REASONABLE CONTROL; (B) DISCLOSURE OF PERSONAL INFORMATION BY THE USER THEMSELVES TO OTHER USERS OR THIRD PARTIES OUTSIDE THE PLATFORM; (C) THE PRIVACY PRACTICES OF THIRD-PARTY WEBSITES OR SERVICES LINKED TO FROM THE PLATFORM; (D) LOSS OF PERSONAL INFORMATION RESULTING FROM THE USER'S OWN ACTIONS OR OMISSIONS, INCLUDING FAILURE TO MAINTAIN SECURE CREDENTIALS; OR (E) INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES RESULTING FROM ANY PRIVACY INCIDENT, EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW.

NETLY's total liability for any privacy-related claim shall not exceed the amounts paid by the affected User to NETLY during the twelve (12) months preceding the incident giving rise to the claim, unless applicable law provides otherwise.

Nothing in this Section limits any mandatory right under Law 25, PIPEDA, or any other applicable legislation that cannot be excluded by contract, nor a Client's rights as a consumer under the Consumer Protection Act (Québec), consistent with Section 13 of the Terms of Use.

ARTICLE 16 — THIRD-PARTY LINKS AND EXTERNAL SERVICES

Websites and services beyond NETLY's control

The NETLY Platform may contain links to external websites, social media platforms, or third-party services. NETLY has no control over the privacy practices, content, or security of these external services and assumes no responsibility for them.

When you leave the NETLY Platform by clicking an external link, this Privacy Policy no longer applies. We encourage you to review the privacy policy of any external service you access. The presence of a link does not constitute an endorsement of that service's privacy practices.

ARTICLE 17 — CONTACT INFORMATION — PRIVACY OFFICER AND COMPLAINT PROCESS

How to reach us and what happens when you do

17.1 Contacting the Privacy Officer

All privacy-related inquiries, requests to exercise rights, and complaints should be directed to NETLY's designated Privacy Officer. This officer has the authority and responsibility to respond to all privacy-related matters on behalf of Vision Concurrence Inc.

Contact method	Details
Email (preferred)	confidentialite@netly.ca — subject line: [Privacy Inquiry / Rights Request / Complaint / Incident Report]
General website	netly.ca/confidentialite
Response time	Acknowledgment within 5 business days; full response within 30 days (extendable to 60 days for complex requests, with notice)

17.2 Complaint handling process

If you have a concern or complaint regarding NETLY's privacy practices, we follow this process:

17. Submission — you submit your complaint in writing to confidentialite@netly.ca, describing the issue and the outcome you are seeking;
18. Acknowledgment — we acknowledge receipt within 5 business days and assign a reference number;
19. Investigation — our Privacy Officer conducts a confidential investigation, which may include reviewing records, consulting relevant team members, and requesting additional information from you;
20. Findings — we communicate our findings to you in writing, including any measures taken or to be taken to address the concern;
21. Corrective measures — where the complaint is well-founded, we implement corrective measures and, where applicable, update our practices;
22. Escalation — if you are not satisfied with our response, we provide you with the information necessary to escalate your complaint to the CAI or the Office of the Privacy Commissioner of Canada.

17.3 Regulatory authorities

You may file a complaint directly with the competent authority at any time:

- Commission d'accès à l'information du Québec (CAI): cai.gouv.qc.ca | 1-888-528-7741 | 525, boul. René-Lévesque Est, Suite 2.36, Québec, QC G1R 5Y4
- Office of the Privacy Commissioner of Canada: priv.gc.ca | 1-800-282-1376 | 30 Victoria Street, Gatineau, QC K1A 1H3

ARTICLE 18 — GOVERNING LAW AND JURISDICTION

The legal framework governing this policy

This Privacy Policy is governed by the laws of the Province of Québec and the applicable federal laws of Canada. Any dispute arising from or relating to this Privacy Policy that is not resolved through the complaint handling process described in Section 17 shall be submitted to the jurisdiction of the courts of the Province of Québec, without prejudice to any User's right to file a complaint with the CAI or the Office of the Privacy Commissioner — consistent with Section 20 of the Terms of Use.

If any provision of this Privacy Policy is found to be invalid, illegal, or unenforceable under applicable law, the remaining provisions shall continue in full force and effect.

NETLY was built on the belief that trust is the foundation of any marketplace. Your personal information is treated with the same care we ask our Service Providers to bring into your home. If anything in this document is unclear, we want to know. Write to us at confidentialite@netly.ca — a real person will respond.

This Privacy Policy takes effect on April 1, 2026 and was last revised on September, 15, 2026.

Document reference: NETLY-PC-2026-EN-v1.2

© 2026 Vision Concurrence Inc., operating as NETLY. All rights reserved.