Privacy Policy

Intelligent Business Concept Inc. Effective date 1 August 2026

This policy explains how Intelligent Business Concept Inc. (we, us or our) handles personal information when you apply for or use our services, visit our website at www.intel-con.com or our platform, or contact us. It explains our purposes, disclosures, retention practices and how you can exercise your privacy rights.

1 Who is responsible for your information

Intelligent Business Concept Inc. was incorporated federally in Canada under the Canada Business Corporations Act on 21 February 2018, under corporation number 1063908-7. The business number shown in its Corporate Profile is 769162280RC0001. Our registered office is 12-30 Wertheim Crt, Richmond Hill, Ontario, L4B 1B9, Canada. We are responsible for personal information under our control and act as a data controller where that terminology applies.

Privacy enquiries and requests: DPO@intel-con.com. You can also contact support@intel-con.com or our platform chat to have a privacy request directed to that team.

We handle personal information under applicable privacy law, including Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA). Applicable provincial privacy laws and other mandatory privacy protections also apply where their legal conditions are met. This policy does not limit those protections.

2 People and services covered

This policy covers individual customers, sole traders, directors, beneficial owners, authorised business users, applicants, payment counterparties and people who contact us. Information about a business is covered to the extent it identifies an individual.

The current services covered are EUR and GBP accounts with virtual IBAN identifiers, incoming and outgoing fiat payments, and foreign exchange through our payment provider, Clear Junction Limited. New services requiring different processing will be explained before that processing begins.

Our individual accounts are available to adults aged 18 or over. We do not offer accounts to minors. Information about a minor may nevertheless appear in supporting records; only information necessary for a lawful purpose should be supplied.

3 Personal information we collect

Identity and contact details: name, date of birth, residential and contact addresses, email, telephone number, nationality, residence and tax residence, identification document details and copies, and identification photographs where required.

Business and compliance information: occupation, business activities, ownership and control, directors and authorised users, source of funds or wealth, expected account activity, supporting invoices and contracts, screening results and due diligence assessments. We also record how you found us and the declarations or supporting information supplied during onboarding.

Account and transaction information: account and virtual IBAN identifiers, balances, amounts, currencies, exchange rates, fees, payment references, sender and beneficiary details, external account details, transaction status, and authorisation records, including OTP verification events.

Technical and communication information: device and browser details, IP addresses, login and security events, authentication information, email correspondence, support chat, complaints, and records of your acceptance of the T&Cs and the applicable Fee Schedule. Customer support does not use telephone calls or video calls; the identity verification video process described below is separate.

Identity verification: we use Sumsub for identity document checks, video liveness and automated comparison of your face with your identification document. These checks use identity images and video and involve biometric processing. Applicable consent or other legal conditions must be satisfied before the check; accepting the T&Cs is not blanket consent to biometric processing.

4 How we obtain information

We obtain information from you through applications, documents, the platform and email or chat. Business customers provide information for business verification (KYB), including relevant representatives and beneficial owners who are subject to identity checks (KYC). We also receive relevant information from senders and beneficiaries, from Clear Junction and other banks involved in a payment, and from Sumsub and other providers performing verification or screening for us.

We may consult official registers, sanctions and politically exposed person databases, fraud prevention sources and relevant publicly available information, including adverse media. Public availability does not remove applicable privacy obligations. We restrict collection to information relevant to the purpose of the check.

When you provide information about another person, you must have a lawful basis to provide it and, where appropriate, give them this policy. This does not transfer our own transparency obligations to you or mean that you can always consent on their behalf.

Information needed to verify identity, understand the customer relationship or process a payment is necessary for those purposes. Without it, we may be unable to open an account or execute a transaction. Optional information and optional consent will be identified separately.

5 Why we use information

Providing services: to assess applications, create and administer accounts, manage authorised users, execute payments and FX instructions, apply agreed fees, handle returns and recalls, and answer service enquiries.

Compliance and security: to verify identity and authority, undertake AML and counter terrorist financing checks, screen for sanctions and other financial crime risks, investigate unusual activity, keep required records, make required reports, and protect accounts and the platform.

Administration and accountability: to resolve complaints and privacy requests, evidence instructions and agreements, maintain accounting records, audit controls and establish, exercise or defend legal claims.

We seek meaningful consent where the applicable law requires it, and rely on statutory permissions or exceptions only where their conditions are satisfied. Acceptance of the T&Cs or acknowledgement of this policy is not blanket consent to every use of personal information.

Where the EU or UK GDPR applies, processing necessary for an individual’s service contract may rely on contractual necessity. Processing concerning business representatives, service security and claims may rely on legitimate interests, subject to necessity and balancing. A legal obligation is relied on only where it qualifies under the applicable framework; a Canadian obligation is not automatically an EU or UK GDPR legal obligation. Consent is used where required. Sensitive or criminal offence information requires any additional legal condition that applies.

6 Risk assessment and automated processing

We use customer information, screening results and transaction activity to assess risk and monitor accounts. Sumsub supports KYC and business onboarding checks and screening for sanctions, politically exposed persons and adverse media. Automated checks can flag unusual activity or reject an instruction that does not satisfy limits or other controls. A failed identity verification results in rejection of the application; you may request human reconsideration by Compliance through support or the privacy contact.

Compliance decides whether enhanced due diligence requires account restrictions or termination. You may question the accuracy of information used, provide relevant clarification and request a review, including human reconsideration of a failed identity verification. We may be unable to explain confidential financial crime indicators or disclosures where the law restricts this.

7 Service messages and marketing

We use contact details for account, security, payment, contractual and regulatory communications. This policy does not authorise promotional campaigns, the sale of personal information, or disclosure to advertisers for their own marketing. Any future optional marketing requires a separately assessed lawful process and any necessary consent. Declining optional marketing will not prevent essential service messages.

8 Who receives information

Payment delivery: we share information needed for payments, FX, due diligence and fraud handling with Clear Junction Limited, banks and other institutions in the payment chain. Relevant transaction information also reaches the sender or beneficiary and their financial institution. A recipient may process information under its own legal duties and privacy notice.

Clear Junction acts as a separate controller to the extent it determines processing for its own legal or regulatory purposes. This data protection role does not make you a direct contractual customer of Clear Junction.

Operational providers: we use Sumsub for identity verification, business onboarding checks and financial crime screening. Verification documents and video remain in Sumsub and are accessible to our authorised personnel for viewing and download through our API integration; they are not automatically copied to our platform storage. We also use providers for platform hosting, maintenance, secure storage, communications and support. Where a provider processes on our behalf, we require confidentiality, appropriate safeguards and processing within our instructions and contractual terms.

Professional and official recipients: information may be disclosed to advisers, auditors, courts, law enforcement, FINTRAC and other competent authorities where required or lawfully permitted. Disclosure is limited to the relevant purpose; it is not based solely on our discretion. We may be prohibited from informing you about a particular disclosure.

Business transactions: relevant information may be shared for a proposed or completed merger, sale or reorganisation only where legally permitted, with confidentiality, purpose limits and any required notice or consent. This is not a general permission to trade customer data.

9 International processing

Our services involve cross border processing. Clear Junction Limited is based in the United Kingdom. Personal information may also be processed or accessed in Canada, the European Economic Area and other countries where relevant service providers or payment institutions operate. Remote access and backup storage are included when assessing these arrangements.

We remain accountable for information processed on our behalf and require appropriate contractual and security safeguards. Foreign courts, law enforcement and public authorities may lawfully access information under local rules. Contracts cannot override those rules.

Where EU or UK international transfer rules apply, we must use an applicable adequacy decision or another valid mechanism, such as the relevant approved contractual safeguards, with any necessary assessment and supplementary measures. We do not assume that Canadian incorporation or encryption alone satisfies those rules. You can contact us for details of the relevant destinations and safeguards, including a copy where applicable, subject to necessary redactions.

10 How long we keep information

We retain information for the service relationship and for the period justified by its purpose and applicable record keeping duties. Different records have different retention periods and starting dates. Closing an account or withdrawing consent does not require deletion of records that must lawfully be retained.

FINTRAC records: many required transaction and internal memorandum records are retained for at least five years from creation. Certain report copies run from submission, and relevant service agreement records run for at least five years from the last transaction. We apply the rule for the particular record, rather than a universal period after account closure.

Complaints: our policy is to retain the complaint file for five years after final closure, including any internal review, unless a longer lawful requirement applies. This is our complaint retention period and is not a universal FINTRAC rule.

Other records: tax and accounting records follow their own statutory periods. Security logs, routine enquiries and unsuccessful or abandoned applications are kept only for a documented period justified by their purpose, legal requirements and relevant claims. Where applicable law requires a minimum period for information used to make a decision affecting an individual, we retain that information for the required period.

Records held by Sumsub remain subject to the applicable purpose and retention rules; external storage does not remove our responsibility for information under our control. Any copies downloaded by authorised staff are subject to the same access and retention controls. A legal hold may extend retention for an investigation, dispute or legal obligation. We review continued retention, restrict access and securely delete or irreversibly anonymise information when no longer required. Backup copies must expire through controlled retention cycles, with deletion controls reapplied after restoration.

11 Security and incidents

We use organisational, technical and physical safeguards appropriate to the sensitivity of the information. Access is limited to authorised people who need it for their work. Our security arrangements include confidentiality obligations, staff guidance and oversight of providers. No system can guarantee absolute security.

We assess suspected privacy incidents, take proportionate containment and remedial action, and notify affected individuals and authorities where required by applicable law. Under PIPEDA, a breach creating a real risk of significant harm must be reported and notified as soon as feasible after that determination. Other applicable rules may impose different thresholds and deadlines. We keep incident records as required.

12 Your privacy rights and requests

You may ask what information we hold about you, how it is used and disclosed, and request access or correction. You may challenge our compliance and withdraw consent where consent is the basis for processing, subject to lawful restrictions. We will explain material consequences, such as being unable to continue a service that needs the information.

Where applicable law provides them, you may also request deletion, restriction or portability, object to processing, and exercise safeguards concerning solely automated decisions with legal or similarly significant effects. These rights have conditions and exceptions; mandatory AML records cannot simply be erased on request.

Send privacy requests to DPO@intel-con.com. We may request proportionate information to verify identity or authority, and will provide a secure way to supply sensitive documents. Do not send passwords or OTP codes. An authorised representative may act with appropriate evidence of authority.

We respond within the period required by the law governing the request. For PIPEDA access requests this is normally 30 calendar days. Where EU or UK GDPR applies, the normal period is one calendar month. Any extension must meet the applicable legal conditions and be notified within the original deadline. Our general complaints timetable does not replace a statutory privacy deadline.

Requests are normally handled without charge. Any exception, fee or refusal must be permitted by the applicable law and explained beforehand where required. We may lawfully withhold information to protect another person's privacy, privilege or an investigation. Where permitted, we explain the reason and how to challenge the response.

You can complain to the Office of the Privacy Commissioner of Canada at www.priv.gc.ca, or the competent provincial privacy authority where its jurisdiction applies. Where relevant, you may also contact the UK Information Commissioner at ico.org.uk or the competent EEA data protection authority, listed at www.edpb.europa.eu/about-edpb/about-edpb/members_en. Our internal process does not remove your right to contact an authority.

13 Website technologies and other websites

We do not use analytics or advertising tracking. Website and platform technologies may support authentication, session security and preferences. Any future optional analytics or tracking must be explained before it begins and used in accordance with applicable requirements, including prior consent where required. This policy alone does not authorise optional tracking.

Other websites and independent providers have their own privacy notices. Read those notices when you use their services. Links do not remove our responsibility for information that remains under our control.

14 Keeping information and this policy up to date

Tell us promptly about relevant changes to your identity, contact details, residence or authority to act for a business. We may request supporting evidence. This does not remove our duty to take reasonable steps to maintain accurate information.

We will date revised versions of this policy and explain material changes through appropriate channels before changed processing begins where required. Any new consent must be obtained separately when necessary. Continued use of an account does not by itself supply consent where express consent is required.