iQuoto

LEGAL DOCUMENT

Privacy Notice.

Version	Effective
1.0	12 October 2026

iQuoto International Limited, trading as iQuoto Global
Registered in St Vincent and the Grenadines · 25708 BC 2019

Privacy Notice.

This notice explains how iQuoto International Limited SVG handles personal information when you apply for an account, use iQ-Trader, make payments or contact us. It covers individuals and the directors, representatives, beneficial owners and other relevant people connected with company and fund clients. It must be provided when information is collected and read alongside any separate provider notice displayed during verification.

CONTENTS

1 Who we are and how to contact us
2 Information covered
3 Sources of information
4 Why information is used
5 Recipients
6 Locations and transfers
7 Calls and communications
8 Retention
9 Your requests and rights
10 Automated processing
11 Security and changes

1 Who we are and how to contact us

1.1 The Company is iQuoto International Limited, incorporated in Saint Vincent and the Grenadines, registration number 25708 BC 2019. Registered office and correspondence address: The Financial Services Centre, P.O. Box 1823, Stoney Ground, Kingstown, St. Vincent & the Grenadines. Website www.iquoto.global. This Company is distinct from iQuoto Limited Mauritius; this notice does not make the Mauritius entity a recipient of your information or the provider of your SVG account.

1.2 Support and Compliance handle privacy requests. Contact compliance@iquoto.global or support@iquoto.global, or write to the address above, marking your message Privacy request. Do not send passwords, full payment-card information or unnecessary identity documents in an initial email; we will arrange proportionate verification securely.

1.3 The Company is responsible as controller for the personal information it determines how and why to process under this notice. Where a provider acts independently for a particular purpose, its applicable notice explains that processing. Any legally required representative or specialist contact can be obtained from Compliance. The use of a UK provider does not determine all laws applying to the Company's processing.

2 Information covered

2.1 Depending on your account and the actual checks required, we may process identity and contact details, date of birth, residence and tax residency, identity and address documents, company or fund authority and beneficial ownership information, financial circumstances and source of funds, payment and transaction records, trading and platform activity, and information you give us in requests or complaints.

2.2 We record calls and retain communications, including relevant messages and complaint correspondence. Platform security records can include login and device information necessary for account access and fraud detection. Data about another person must be supplied only with lawful authority and appropriate information to that person.

2.3 Identity verification is undertaken through Sumsub using the checks relevant to your application and legal requirements. Where checks require document images, selfies, liveness or biometric information, sanctions or politically exposed person screening, the verification flow supplies the relevant information and any consent or authorisation required before processing. We do not require unrelated sensitive data merely because a provider offers an optional feature.

3 Sources of information

3.1 Information is provided by you, your authorised representative, or a company or fund for which you act. We may also receive information necessary for payments and identity checks from banks, payment service providers and Sumsub, and relevant publicly available or official verification sources. We will not obtain unrelated employer, credit or other personal information without a relevant lawful purpose.

4 Why information is used

4.1 We use information to assess and administer applications, verify identity and authority, maintain accounts, execute and record transactions, process deposits and withdrawals, communicate about services, investigate complaints and privacy requests, prevent fraud and financial crime, meet applicable recordkeeping and reporting requirements and establish or defend lawful claims.

4.2 Where applicable law requires a legal basis, account administration and transaction processing rely on necessary contract performance; legally required identity, financial-crime and reporting activities rely on the relevant legal obligations; proportionate security, complaint investigation and claims handling may rely on properly assessed legitimate interests where law permits; and optional or sensitive-data processing uses valid consent or another specifically applicable lawful basis. We explain the relevant basis and purpose and do not treat acceptance of trading terms as unlimited consent.

4.3 Required identity and payment information may be necessary to open or operate an account lawfully. If it is not supplied, we may be unable to provide the relevant service. We will distinguish required information from optional uses. Refusal of optional marketing consent must not be treated as refusal to provide essential identity information.

4.4 Marketing, optional social features, public trader or follower profiles and non-essential website tracking require their own applicable disclosures and choice or legal basis. This notice does not authorise unlimited advertising use or sale of client information.

5 Recipients

5.1 Access within the Company is limited to personnel who need information for their work, including Support and Compliance for requests and complaints and relevant operational teams for account and payment administration. Appropriate access controls and confidentiality must apply.

5.2 Confirmed external recipient categories are banks, payment service providers and KYC companies. The Company has identified Steven AB in Sweden as its XOALA payment provider and SettleGo Solutions Limited in England as its OpenPayd provider. The information shared must be necessary for the particular payment, account or legal function. Their regulatory status does not make them the Company's brokerage regulator or provide a general permission to disclose all data.

5.3 Sumsub is the identified KYC provider. Its published notices identify Sum and Substance Ltd, English company number 09688671, and relevant group entities. The verification flow identifies the applicable service notice and processing role, including any purpose for which Sumsub acts as an independent controller. Its selected verification services and any authorised subprocessors are governed by the accepted provider arrangements; necessary consent or information is supplied before a check. Details of the applicable provider arrangement and processing locations can be requested from Compliance.

5.4 We may provide necessary information to competent authorities when lawfully required, and to legal or professional advisers where genuinely necessary and lawful. Affiliates, independent traders and liquidity providers are not automatically given unrestricted client information. Disclose any actual sharing with them, including categories and purposes, before relevant processing; a shared brand or a copied strategy does not itself establish a lawful basis.

5.5 A prospective transfer of the client relationship does not create unlimited authority to disclose or move personal information. Any necessary due diligence or transfer must meet applicable law, use appropriate safeguards and provide required notice. The account agreement cannot waive non-excludable privacy duties.

6 Locations and transfers

6.1 The Company is registered in SVG and uses identified payment providers in Sweden and England and the UK-based Sumsub KYC service. Processing can involve provider group companies, authorised subprocessors and staff or infrastructure in other locations under the applicable arrangements. Provider headquarters are not a promise that all data stays in that country. Contact Compliance for relevant location and safeguard information.

6.2 Where applicable law restricts an international transfer, we must identify and implement the required lawful mechanism and safeguards, including any relevant contractual measures, assessments or permissions. You may request information about applicable safeguards, subject to appropriate confidentiality and legal limits.

7 Calls and communications

7.1 Calls are recorded for transaction evidence, account security, service monitoring, complaint investigation and compliance purposes where necessary and lawful. We will provide required recording information and obtain any necessary consent before recording. This notice is not a waiver of recording laws in other applicable jurisdictions.

7.2 Relevant recordings and communications may be reviewed by authorised staff and supplied in response to lawful requests, subject to identity checks, third-party privacy and legally required restrictions. The Company must preserve records relevant to an actual or reasonably anticipated dispute even where ordinary disposal would otherwise be scheduled.

8 Retention

8.1 Calls and other communications are retained for seven years from the relevant event. For a call this is the recording date; for a message it is the recorded sent or received date. Relevant material is preserved longer where a lawful hold or actual or reasonably anticipated dispute requires it. This is the Company's communications policy, not a universal statutory period for all data.

8.2 Identity/KYC, account, trading, payment, security, complaint and privacy-request records are retained for the period justified by the relevant service, applicable legal requirements, audit and financial-crime obligations or lawful claims. The criteria include the account relationship, transaction or verification date, any applicable statutory period and a required legal hold. Communication retention does not automatically require every biometric template to be kept seven years. Compliance can explain the applicable category period and criteria on request.

8.3 At the end of the applicable period, information must be securely deleted or appropriately anonymised, subject to required backup cycles and legal holds. Providers' retention periods and roles must be addressed under their accepted agreements and applicable notices; our seven-year communications policy does not prove their period or override their lawful obligations.

9 Your requests and rights

9.1 Support and Compliance will receive requests concerning information held about you, including access and correction. Depending on applicable law and circumstances, rights may also include deletion, restriction, objection, portability or withdrawal of consent. These are not unconditional promises that all data can be deleted or that every statutory right applies in every jurisdiction.

9.2 Explain the requested action and relevant account or event. We may make proportionate identity checks without seeking excessive information. We will respond within the applicable legal period, explain any lawful restriction and provide an available review route. A privacy request is not itself a trading Default and must not be used to withhold unrelated available funds.

9.3 Withdrawal of consent, where consent is the actual basis, does not invalidate earlier lawful processing. We may retain or process information on another valid basis where applicable law permits or requires it. Optional marketing preferences may be changed without closing a trading account.

9.4 You may complain to compliance@iquoto.global under our Complaints Policy, without losing any right to approach a competent privacy authority or court. These terms do not promise ICO jurisdiction solely because Sumsub or a payment provider is UK-based.

10 Automated processing

10.1 KYC screening and security processes use automated tools where appropriate. The relevant verification or service disclosure explains any automated decision requiring particular information or safeguards under applicable law, including the effect and available review route. Contact Compliance for a lawful review request. Automated trade copying and privacy-law automated decision-making are separate classifications.

10.2 Where a relevant review right applies, contact Support or Compliance. Identity-screening results must be handled through the approved review and escalation process, with appropriate legal restrictions on revealing suspicious-activity reports or sensitive security methods.

11 Security and changes

11.1 We will apply appropriate technical and organisational controls, proportionate to the information and risks, including access restrictions and secure transmission and retention arrangements. No system is guaranteed immune from attack. Where a security incident triggers notification duties, we will follow applicable law and the approved incident process.

11.2 Material changes to how we use personal information will be communicated as required by law before new processing where necessary. A revised notice cannot retrospectively legitimise processing or replace required consent. The published notice must state its version and effective date and remain

available in a retainable form.

iQuoto

Questions about this document?

Support

support@iquoto.global

Compliance and complaints

compliance@iquoto.global

Website

iquoto.global

Client portal

secure.iquoto.global

---

iQuoto International Limited, trading as iQuoto Global. An International Business Company incorporated in St Vincent and the Grenadines, registration number 25708 BC 2019.

Registered office and correspondence address: The Financial Services Centre, P.O. Box 1823, Stoney Ground, Kingstown, St. Vincent & the Grenadines.

Risk warning. FX and CFDs are complex, leveraged financial products which carry a high level of risk to your capital. Trading on margin can result in losses that exceed your deposits, and these products are not suitable for all investors. You should ensure you fully understand the risks involved, and seek independent advice if necessary, before opening an account. Past performance is not a reliable indicator of future results.

© 2026 iQuoto International Limited