Conneqtid Privacy Notice

Corporate information

Conneqtid Curaçao B.V. and Conneqtid VBA (together "Conneqtid", "we", or "us") provide anti-money laundering and counter-terrorist financing (AML/CFT) onboarding software that helps organizations meet their AML/CFT obligations.

Our company information:

- Conneqtid Curaçao B.V., a limited liability company, registered at the Chamber of Commerce of Curaçao under number 162614, with its office at Scharlooweg 102, Willemstad, Curaçao.
- Conneqtid VBA, a limited liability company, registered at the Chamber of Commerce of Aruba under number H55125.0, with its office at Italiestraat 38 unit 9, Oranjestad, Aruba.

What does Conneqtid do?

Conneqtid is a platform service provider. Our clients, such as real estate agents, brokers, project developers and car dealers ("Clients"), are organizations with AML/CFT obligations. They use our platform to identify and verify their own customers, check the source of funds, assess risk, and complete transactions with other parties such as notaries.

Conneqtid does not provide AML/CFT compliance services itself[1]. We do not carry out customer due diligence on behalf of our Clients, decide whether a customer is accepted, or report to authorities; these remain the Client's own obligations and decisions. Within the platform, we offer a screening service[2] that Clients can use as part of their own due diligence.

Clients use the platform under their agreement with Conneqtid. Each Client remains responsible for the customer checks it carries out and the decisions it makes.

Our role: processor and controller

We handle personal data in two capacities:

- **As a Data Processor:** when a Client uses our platform to identify and verify its customers (and related persons such as beneficial owners and representatives), we process that personal data on behalf of the Client, based on our agreement with the Client. The Client is the data controller, and the Client's own privacy notice applies to that processing.
- **As a Data Controller:** for our own business purposes, we decide how personal data is processed. This covers visitors to our website, people who contact us, contact persons at our (prospective) Clients, and Client employees who hold a user account on our platform.

This notice explains both. Where a section applies to only one role, it says so. If you are a customer of one of our Clients, please read the Client's privacy notice first, as the Client is responsible for the processing of your data.

Conneqtid does not keep customer data for reuse by other Clients

We do not keep customer data for our own purposes. When a Client's use of the data ends, the data is retained or deleted in line with our agreement with the Client (see Section 7). Where a Client offers its customers the option to store their data within the Client's environment for future transactions, the Client does so with the customer's consent.

[1]Conneqtid may provide outsourced compliance officers to Clients as a secondary service. These officers act under the responsibility of the respective Client.
[2]This screening service is provided under the brand name Stracket.

Conneqtid's commitment to data privacy

We are committed to protecting your privacy and handling personal data transparently and securely. Nothing in this Notice limits your rights under the applicable data privacy laws ("Data Privacy Laws"):

- Aruba: Landsverordening Persoonsregistratie (AB 2011 no. 37)
- BES Islands: Wet Bescherming persoonsgegevens BES
- Curaçao: Landsverordening Bescherming Persoonsgegevens (LBP) A.B. 2010, nr. 84

This Notice comes into effect on 01 January 2027.

1. How can you contact us?

For personal data that we process as a Data Processor on behalf of a Client, please contact that Client directly.

For all other questions, concerns, or to exercise your rights, contact our Privacy Officer at:

- Email: info@conneqtid.com
- Post: Privacy Officer, Conneqtid Curaçao B.V., Scharlooweg 102, Willemstad, Curaçao

We respond within four weeks, in accordance with the applicable Data Privacy Laws.

2. What kind of personal data do we process, and how?

"Personal Data" means any information about an identified or identifiable individual.

2.1 Data we process on behalf of Clients

Clients use the platform to collect the following data from their customers and related persons:

Category	Examples
Customer identification data	• Full name • Email • Phone number • Address • Passport/ID information • Other identifiers
Beneficial owner and representative data	• Data on beneficial owners, shareholders and representatives of legal entities, including ownership percentage and position
Source of funds	• Information and documents on the origin of the funds used in the transaction
Financial and transaction data	• Bank details • Transaction details, such as the property or object, price and currency
Signature data	• Typed name, drawn signature and signing date
Risk data	• Initial and overall risk rating • Compliance review notes and remarks
Screening and verification data	• Screening data • Adverse media results • Public news sources
Regulatory reporting data	• Reports to the Financial Intelligence Unit (FIU), where the Client uses the platform to prepare them

This data is provided by the Client, by you at the Client's request (for example through an onboarding link), or obtained from screening sources and public registers as part of the Client's onboarding process. The platform requests the data needed to meet AML/CFT requirements. By using the platform, the Client accepts these data fields as necessary for its own obligations.

We treat identity documents and screening results as sensitive. Access is restricted to authorized users of the relevant Client and to Conneqtid staff who need it to provide the service.

We do not intentionally collect special categories of personal data. Identity documents may incidentally reveal ethnic origin, and screening may reveal political affiliation or information on criminal offences; this data is processed only as far as AML/CFT laws require.

2.2 Data we process as a Data Controller

Category	Examples
Platform and access data	• Platform user account name • Authentication data (including MFA tokens) • Audit logs
Client contact data	• Name, job title, business email and phone number of contact persons at Clients and prospective Clients
Website and marketing data	• Contact form inquiries • Cookie and analytics data

We collect this data directly from you, from the Client that employs you, or through your use of our website and platform.

3. What do we use personal data for?

As a Data Processor

We carry out the following activities on behalf of Clients, as part of the service agreed with them:

- **AML/CFT checks for our Clients:** risk assessment and screening against sanctions lists, PEP lists, and adverse media.
- **Completing transactions:** making verified information available to other parties involved in a transaction, such as a notary, where the Client uses this function.

As a Data Controller

- **Providing our services:** setting up and managing platform user accounts and our relationship with Clients.
- **Security and compliance:** maintaining the security of our platform, keeping audit logs, and complying with legal obligations.
- **Website and communication:** answering contact-form questions and improving our website.

4. What is our legal basis for handling your personal data?

When we act as a Data Processor, the Client determines the legal basis, which is generally the Client's legal obligation under AML/CFT laws, and we process the data under our agreement with the Client.

When we act as a Data Controller, we rely on:

- **Contractual agreements:** to provide our services to Clients and platform users.
- **Legal obligations:** to respond to authorities.
- **Legitimate interests:** to secure the platform and answer contact-form questions.
- **Consent:** for analytics cookies.

5. Who do we share your personal data with?

- **Parties to a transaction:** other parties involved in a Client's transaction, such as a notary, where the Client uses the platform to share it.
- **Service providers:** hosting, cloud infrastructure, and analytics providers that support our platform and website, including DigitalOcean (United States) for platform and database hosting, Google Cloud (United States and Belgium) for document storage and PDF generation, SendGrid (United States) for email, Bravobit (the Netherlands) for platform development, and Gravity Forms for our website contact form.
- **Authorities:** when required by law or in response to a valid legal request (for example, regulatory enforcement).
- **Business transfers:** in a merger or acquisition, to the acquiring party, subject to this Notice.

We do not sell personal data.

6. Where in the world is personal data sent and stored?

Conneqtid uses cloud service providers primarily located in the United States. For certain services, data is processed in Belgium and the Netherlands. This applies to data we hold for ourselves and data we hold on behalf of Clients.

Our main US providers, Google and DigitalOcean, are certified under the EU-U.S. Data Privacy Framework.

7. How long is personal data retained?

As a Data Processor: we retain data in line with our agreement with the Client and the retention periods that apply to the Client under AML/CFT laws. When our agreement with the Client ends, we return or delete the data as agreed in the data processing agreement, unless the law requires us to keep it.

As a Data Controller: we retain data for as long as needed for the purpose for which we collected it, or as required by law. Retention periods range from 5 to 10 years, depending on the type of information and the profile of the Client.

Once retention is no longer required, we take reasonable steps to destroy or de-identify the information in accordance with the applicable Data Privacy Laws. Deleted data may remain in backups for up to 28 days before it is overwritten.

8. Do we make automated decisions about you?

Risk ratings and screening results generated by the platform are tools for the Client's own assessment. The Client reviews them and makes the final decision. Conneqtid does not make decisions about you with legal or similarly significant effect based solely on automated processing. Risk ratings are calculated with a documented, explainable formula using the data in Section 2.1. You may ask the Client for an explanation of how a risk rating was produced, ask for human review, give your point of view, and contest it with the Client.

9. How do we handle data of minors?

Our services are not directed at children (persons under 18). Where a minor is subject to verification (for example as a beneficiary or party to a transaction), their data is processed only as part of the Client's onboarding process and, where required, with the consent of a parent or legal guardian.

10. What rights do you have?

You have rights under the respective Data Privacy Laws. Where we act as Data Controller, you can ask us to access, correct, complete, delete, or block your personal data. You can also object

to processing based on our legitimate interest, object to direct marketing at any time, and withdraw consent where you gave it. Where the applicable law provides for it, you can also ask us to restrict processing or to provide your data in a portable format. Requests are free of charge. Some rights are limited by AML/CFT laws; for example, data a Client must keep cannot be deleted early. We respond in writing within four weeks. Requests can be sent to us (see Section 1). We may ask you to verify your identity. You can also lodge a complaint (see Section 12).

For personal data we hold as a Data Processor on behalf of a Client, please contact the relevant Client. We will support the Client in responding.

11. Security

We use appropriate physical, technical, organizational, and administrative measures to protect personal data from unauthorized access, use, and disclosure. Key safeguards include:

- **Encryption:** all data is encrypted in transit using TLS 1.2 or higher, and stored documents are encrypted at rest.
- **Infrastructure:** hosting is provided by organizations that hold either ISO 27001 certification or a SOC 2 Type 2 attestation.
- **Access controls:** portal access is protected by multi-factor authentication: sign-ins from a new or unrecognized browser require a verification code sent by email. Passwords are stored in hashed form, access within the platform is role-based, and each Client's environment is separated from those of other Clients.
- **Documents:** documents are not publicly accessible and can only be opened through short-lived secure links.
- **Backups:** the database is backed up twice a day, and backups are kept for 28 days.
- **FIU reports:** reports prepared through the platform for the FIU are encrypted before they are sent.
- **Penetration testing:** we engage qualified third parties to perform periodic penetration testing of our platform and APIs. Findings from the most recent test were confirmed as remediated in a retest.

While we take measures to protect the information we hold, no method of transmission or storage is ever completely secure. These measures apply equally to data we hold on behalf of Clients.

If a security incident affects personal data we hold on behalf of a Client, we inform that Client without undue delay.

12. Who can you complain to?

For data we process as a Data Processor, please direct complaints to the relevant Client. For data we process as a Data Controller, please contact us first (see Section 1).

If you are unsatisfied, you can contact:

- Aruba: Aruba has no independent data protection authority. Violations of the Landsverordening persoonsregistratie can be reported to the Public Prosecutor's Office (Openbaar Ministerie) of Aruba, and you may seek a remedy through the courts.
- BES Islands: Commissie Toezicht Bescherming Persoonsgegevens BES
- Curaçao: College Bescherming Persoonsgegevens

13. Cookies

Our website uses cookies and similar technologies. These fall into two types:

- **Strictly necessary cookies:** required for the website and platform to work, such as keeping you securely logged in. These cannot be switched off.
- **Analytics cookies:** help us understand how visitors use our website so we can improve it. We use Google Analytics 4, provided by Google. These cookies are kept for up to two

years in your browser. The analytics data collected through them is kept in Google Analytics for two months.

We do not use cookies for advertising. Non-essential cookies are only placed with your consent, which you can withdraw at any time via your browser settings.

14. Changes to this Privacy Notice

We may update this Notice from time to time. The effective date at the top shows the current version. For material changes, we will notify Clients and, where we hold your contact details as Data Controller, inform you directly before the change takes effect. Material changes are changes that affect how we use your data or your rights. We announce them by email to Clients and by a notice on our website.