TERMS AND CONDITIONS

VEYCO LTD

19 January 2026

Table of Contents

Veyco

SECTION 1 — DEFINITIONS AND INTERPRETATION

1.1 Definitions

In these Terms, the following words and expressions have the meanings set out below. These definitions apply whether the words appear in the singular or plural and regardless of capitalisation. Headings are for convenience only.

"Account"

means a Partner or User account used to access the Platform, whether through a username/password, secure link, API key, or other authentication method.

"Affiliate"

means any entity that directly or indirectly controls, is controlled by, or is under common control with another entity, where "control" means ownership of at least 50% of voting rights.

"AI/ML Restrictions"

means the obligations preventing any Partner or User from using any data, outputs, verification results, Referencing Information, or Reports to train, test, benchmark, evaluate, or compare AI or machine-learning models.

"AISP"

means an Account Information Service Provider that is authorised by the Financial Conduct Authority to access payment account data under the Open Banking framework.

"AML Laws"

means the Money Laundering Regulations 2017 (as amended), Proceeds of Crime Act 2002, Sanctions and Anti-Money Laundering Act 2018, and all equivalent legislation relating to anti-money laundering, counter-terrorist financing, sanctions, and anti-fraud.

"API"

means the application programming interface, API keys, endpoints, documentation, sample code, webhooks, and all other materials through which Veyco makes parts of the Services programmatically accessible.

"Applicable Law"

means all laws, regulations, statutory requirements, regulatory guidance, codes of practice, case law, and industry standards that apply to a party or to the processing of data or provision of the Services, including UK GDPR, the Data Protection Act 2018, PECR, the Immigration Acts, Consumer Rights Act 2015, Companies Act 2006, and the retained UK eIDAS Regulation.

“Audit Trail”

means the record of events, metadata, logs, timestamps, device data, IP addresses, cryptographic evidence, certificate details, and historical signatures generated in relation to identity verification or electronic signing processes.

“Biometric Data”

means personal data resulting from specific technical processing relating to a person’s physical, biological, or behavioural characteristics, such as facial images, liveness indicators, and face-match vectors, which allow unique identification.

“Business Customer”

means a Partner or enterprise client using the Platform for business purposes.

“Business Day”

means Monday to Friday, excluding UK public holidays.

“Certificate” or “Signature Certificate”

means the formal digital certificate generated during a Qualified Electronic Signature (QES) process, containing signer identity information, timestamps, verification results, and cryptographic proof of signature validity.

“Confidential Information”

means all confidential, proprietary, or commercially sensitive information disclosed by one party to the other, including Platform details, processing methods, Reports, pricing, client lists, security processes, and any technical or operational information not publicly known.

“Content”

means text, images, documents, signatures, videos, data, and other materials submitted, uploaded, or generated through the Platform.

“Controller”, “Processor”, “Data Subject”, “Personal Data”, “Processing”

have the meanings given in the UK GDPR.

“Credit Check”

means a search of a credit reference agency’s database relating to a User. For the avoidance of doubt, **Veyco does NOT perform credit checks**.

“Data Incident”

means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed by Veyco.

“Data Protection Laws”

means all data protection and privacy laws applicable in the UK, including UK GDPR, the Data Protection Act 2018, and PECR.

“Device Check”

means an assessment of the User’s device, browser, IP address, timezone, and related technical attributes for fraud-prevention and identity-verification purposes.

“Document Verification”

means verifying the authenticity of documents such as passports, driving licences, visas, payslips, bank statements, utility bills, tenancy agreements, guarantor documents, and other supporting materials.

“Electronic Signature Services”

means Veyco’s Qualified Electronic Signature tools, signature workflows, certificate generation processes, and associated Audit Trails.

“Employment Verification”

means confirmation checks relating to a User’s employment or contractor status as part of Tenancy Referencing Services.

“Fees”

means all charges payable for the Services, as agreed in writing or displayed at the point of purchase.

“Guarantor Information”

means information about a guarantor provided during tenancy referencing, including identity documents, contact details, income documents, and supporting materials.

“Identity Verification Services”

means any service designed to verify the identity of a User, including biometric checks, face-match, liveness detection, document checks, Device Checks, and risk-based assessment workflows.

“Indemnified Claim”

means a claim brought against Veyco that arises from (i) a Partner’s breach of these Terms; (ii) their unlawful or incorrect instructions; or (iii) misuse of the Platform.

“Liveness Detection”

means technology used to determine whether a real human is present during a selfie or video capture, designed to detect spoofing or fraudulent attempts.

“Open Banking Services”

means services using the UK Open Banking standard to access User financial data via account-information service providers.

“Partner”

means any legal entity or organisation using the Platform for business purposes, including but not limited to letting agents, landlords, estate agents, property managers, build-to-rent operators, brokers, law firms, conveyancers, software providers, or other commercial users.

“Partner Dashboard”

means the secure online interface through which Partners access Reports, initiate identity checks, manage workflows, and view audit data.

“Personal Data Breach”

has the meaning given in the UK GDPR.

“Platform”

means the software, systems, website(s), portals, APIs, dashboards, and related tools owned or operated by Veyco and accessible via veyco.com, or via the app.

“Qualified Electronic Signature” or “QES”

means an electronic signature that satisfies the requirements of the UK eIDAS Regulation (as retained in UK law), supported by identity verification and issued using a valid digital certificate.

“Referencing Information”

means all data collected or supplied for Tenancy Referencing Services, including employment information, tenancy history, bank statements, guarantor information, and other supporting documentation.

“Reports”

means any output produced by the Services, including identity verification results, referencing assessments, risk flags, signature certificates, and audit outputs.

“Right to Rent Checks”

means checks required under the Immigration Act 2014 relating to whether a person has the right to reside in the UK.

“Services”

means the full set of services offered by Veyco, including identity verification, biometric processing, document verification, tenancy referencing, QES, Reports, dashboards, APIs, and customer support.

“Sub-Processor”

means any third party engaged by Veyco to process Personal Data on its behalf.

“Tenancy Referencing Services”

means the assessment tools, workflows, and data processing used to help Partners evaluate a User’s suitability for a tenancy.

“User”

means an individual using the Platform at the request of a Partner or accessing verification or signing workflows.

“Verification Data”

means all data collected, submitted, or generated through identity verification, referencing, or signing workflows, including:documents, biometrics, images, videos, device information, and risk signals.

SECTION 2 — SCOPE OF SERVICES

2.1 Overview of the Services

Veyco provides a set of technology tools designed to support identity verification, document checks, biometric analysis, tenancy referencing, electronic signatures and related compliance workflows.

The Services include:

- **Identity Verification Services**
- **Document Verification**
- **Tenancy Referencing Services**
- **Qualified Electronic Signature (QES) Services**
- **Audit Trails and Evidence Files**
- **Partner Dashboard access**
- **API access (where applicable)**
- **Secure document storage**
- **Right to Rent workflows (where applicable)**

These Services are supported by third-party technology providers, compliance databases, document analysis engines, biometric engines and certificate authorities.

2.2 What Veyco's Services Are (and Are Not)

Veyco provides **tools** that help Partners confirm identity, assess suitability and execute legally binding electronic signatures.

Veyco does provide:

- Systems to collect information from Users
- Identity and document verification workflows
- Biometric checks (face-match, liveness)
- Tenancy referencing processing
- QES and signature audit trails
- Reports that summarise checks performed
- Secure storage and retrieval of verification data
- Tools for Right to Rent evidence capture
- Fraud-risk and device-integrity checks
- Partner dashboards and API integrations

Veyco does not provide:

- Legal advice
- Tenancy suitability decisions
- A guarantee that identity or documents are genuine
- A guarantee that Users will meet any tenancy obligations
- A guarantee that referencing information is correct or complete
- Any credit-checking services
- Any immigration advice or status determinations
- Any responsibility for tenancy agreements uploaded by Partners
- Any obligation to pursue or enforce tenancy breaches

Partners remain **entirely responsible** for decisions they make using Reports.

2.3 Identity Verification Services

Identity Verification Services may include:

1. **Document verification**
    - Passport analysis
    - Driving licence checks
    - Residence permit checks
    - Other photo-ID validation
    - Detection of tampering, hologram issues, MRZ errors, or data mismatches
2. **Biometric verification**
    - Face-match comparison
    - Liveness detection to prevent spoofing
    - Assessment of facial similarity scores
3. **Third-party database checks**
    - Sanctions lists (if enabled)
    - Politically exposed persons (PEP) lists (if enabled)
    - Fraud-prevention and identity-assurance services
4. **Audit Trails**
   Logs of actions, captures, timestamps, device attributes, certificate events and risk assessments.

Veyco may update, enhance or modify verification methods at any time to reflect industry standards or security needs.

2.4 Tenancy Referencing Services

Veyco provides a suite of tools to assist Partners in assessing User suitability for a tenancy.

These tools may include:

- Collection of employment information
- Collection of income, payslips or financial data
- Analysis of affordability (based on supplied information)
- Collection of tenancy history or landlord references
- Collection of guarantor information
- Validating Right to Rent documentation
- Fraud-risk signals and document consistency checks

Important points:

- Veyco **does not perform credit checks**.
- Veyco's role is to **collect and process information**, not to advise on tenancy decisions.
- Reports are **support tools** only; they do not guarantee outcome or suitability.

Partners remain responsible for:

- the decision to accept or reject a User
- setting referencing policies
- complying with the Immigration Acts, landlord regulations, and other legal obligations.

2.4A Open Banking Services

2.4A.1 Overview

As part of its Tenancy Referencing Services, Veyco may enable the use of Open Banking technology to allow Users, at the Partner's request, to securely share certain financial account information for referencing and affordability assessment purposes ("Open Banking Services").

2.4A.2 Nature of the Service

Open Banking Services are used solely to:

- verify income and affordability information supplied by the User;
- assess transaction history relevant to tenancy referencing; and
- support fraud-prevention and consistency checks.

For the avoidance of doubt, Open Banking Services:

- do not involve credit scoring or credit checks;
- do not provide lending decisions or financial advice; and
- do not guarantee affordability, suitability or payment behaviour.

2.4A.3 Third-Party Providers

Open Banking Services are delivered using FCA-authorised Open Banking providers and AISPs. Veyco does not itself hold banking licences and does not access User accounts directly.

2.4A.4 User Consent

Users must provide explicit consent before any Open Banking data is accessed. Consent is time-limited, revocable, and managed through the relevant Open Banking provider.

2.4A.5 Partner Responsibility

Partners remain solely responsible for:

- determining whether Open Banking information is required;
- interpreting Open Banking outputs;
- making any tenancy or affordability decisions; and
- complying with landlord, consumer and housing law.

Open Banking data is provided as a support tool only.

2.5 Electronic Signature Services – Qualified Electronic Signature (QES)

Veyco provides **Qualified Electronic Signature** services designed to comply with:

- the **Electronic Communications Act 2000**; and
- the **UK retained eIDAS Regulation**.

QES Services may include:

- user identity verification
- cryptographic signature generation
- issuance of signature certificates
- signature timestamping
- binding audit trails
- confirmation of signer identity
- secure storage and retrieval of signed documents

Legal effect:

A QES created through Veyco is intended to carry the **same legal effect as a handwritten signature**, to the extent permitted by law.

Important responsibilities:

- Veyco is **not a party** to any signed agreement.
- Veyco does **not approve, validate or review** Partner-supplied documents.
- Partners must ensure their documents are **legally compliant** and **suitable**.

2.6 API Access & Integrations

Where API access is provided, Partners may use the API to:

- trigger identity checks
- retrieve verification results
- embed journeys into their own applications
- automate referencing workflows

API usage is subject to:

- API keys
- rate limits
- security requirements
- strict use-case restrictions
- anti-AI-training restrictions

Veyco may suspend API access if the Partner breaches security rules, misuses data or overloads the system.

2.7 Reports and Outputs

Reports may include:

- verification outcomes
- referencing assessments
- auditing information
- signature certificates
- Right to Rent check summaries
- fraud-risk indicators

These Reports are **informational only**. They **do not constitute legal, financial or tenancy advice**.

Partners must:

- interpret Reports responsibly,
- consider additional information as necessary, and
- make their own decisions.

Veyco is **not responsible** for any actions taken based on a Report.

2.8 Availability of the Services

Veyco aims to keep the Platform running reliably and securely but does **not** guarantee:

- uninterrupted availability
- freedom from errors or defects
- zero downtime
- compatibility with all devices or browsers

Veyco may:

- perform maintenance,
- update the Platform,
- patch security vulnerabilities,
- remove outdated features, or
- change integrations

without liability to Users or Partners, provided such changes do not substantially impair core functionality.

2.9 Prohibited Uses of the Services

You must **not**:

1. use the Platform to commit or facilitate fraud
2. submit falsified documents or information
3. interfere with or disable security systems
4. scrape, harvest or extract data
5. benchmark Veyco against competitors
6. use Veyco data for AI training
7. use the Platform for unlawful tenancy discrimination
8. upload copyrighted or illegal material
9. run automated or scripted submissions without permission

Violation of these rules may result in:

- suspension,
- termination,
- reporting to authorities, or
- legal action.

2.10 No Professional Advice

Veyco does not provide:

- legal or financial advice
- tenancy suitability assessments
- immigration or Right to Rent advice
- employment verification advice

All decisions remain the responsibility of the Partner.

2.11 Changes to the Scope of Services

Veyco may:

- update verification methods,
- add new services,
- discontinue older features,
- modify technical workflows,
- introduce new API versions

as required for security, legal compliance, or service improvement.

Significant changes will be communicated to Partners in advance where reasonably possible.

SECTION 3 — IDENTITY VERIFICATION & BIOMETRIC PROCESSING

3.1 Overview of Identity Verification Services

Veyco provides Identity Verification Services to help Partners confirm the identity of Users. These services may include:

- document authenticity checks
- biometric analysis (face-match)
- liveness detection
- device and IP checks
- database lookups (if enabled by the Partner)
- Right to Rent evidence collection
- fraud-detection signals
- audit trail generation

Identity Verification Services are designed to reduce risk but **cannot guarantee** that:

- a User is who they claim to be;
- documents provided are genuine or unaltered; or
- a User will satisfy legal or contractual obligations.

3.2 Identity Verification Workflow

Verification flows may include:

1. **Capture of identity documents**
   Users may be asked to upload or photograph identity documents such as a passport, driving licence, or residence permit.
2. **Optical and data-centric checks**
   Veyco or its verification providers may analyse:
   - document integrity
   - hologram behaviour
   - MRZ consistency
   - barcode data
   - NFC chip data (if available)
   - expiry dates and issuing authority information
3. **Image and video capture**
   Users may be required to take a selfie, record a short video, or perform specific movements.
4. **Biometric comparison**

Biometric engines compare the User's live capture with their identity document photo.

5. **Liveness detection**
   Tests designed to confirm the User is a real human, not a recording, mask or spoof attempt.
6. **Device and environmental checks**
   Includes IP address, timezone, device fingerprinting, pixel anomalies and additional risk factors.
7. **Result generation**
   The Platform generates a Report summarising:
   - pass/fail results
   - confidence scores
   - fraud-risk indicators
   - document inconsistencies
   - metadata

All such results are for **informational purposes only**.

3.3 Biometric Data Processing

Biometric Data is processed **only where permitted** under Data Protection Laws and may be used for:

- verifying identity
- liveness detection
- detecting fraud and spoofing
- Right to Rent checks (where biometric verification is used)
- QES identity validation
- ensuring integrity of verification processes

Veyco processes Biometric Data on:

(a) Explicit consent

Users give clear, explicit consent before their biometric data is processed.

(b) Substantial public interest

For certain checks (e.g., Right to Rent or fraud prevention), processing may also rely on the substantial public interest condition under the Data Protection Act 2018.

(c) Legitimate interests

For device fraud detection and identifying duplicate accounts, where appropriate.

Veyco does **not** use biometric data for:

- marketing
- profiling unrelated to verification
- any automated decision-making with legal effects
- AI model training
- sharing with unrelated third parties

3.4 Limitations of Identity Verification

Identity Verification may fail or be inaccurate due to:

- poor image quality
- lighting and environmental issues
- damaged or non-standard documents
- real faces that do not meet liveness thresholds
- false positives or false negatives in biometric systems
- document forgeries that evade automated detection
- inconsistent or incorrect Issuing Authority information
- mismatched data provided by third parties

Veyco does **not** guarantee:

- that every fraudulent document will be detected;
- that biometric engines will always be correct;
- continuous availability of verification providers; or
- that identity verification is suitable for any particular purpose.

Partners must use their **own judgement** when interpreting results.

3.5 Device Intelligence & Fraud Prevention Checks

Veyco may use device-level intelligence to detect:

- high-risk VPNs or proxies
- known fraud devices
- velocity patterns (multiple attempts)
- impossible travel events
- tampering, manipulation or replay attacks
- unusual user-agent behaviour

These indicators are provided **for fraud-prevention purposes only**.
They do **not** represent definitive findings.

3.6 Document Verification & Supporting Materials

Users may be required to upload supporting documents, which may include:

- payslips
- bank statements
- employment letters
- guarantor documents
- utility bills
- tenancy agreements
- proof of address
- immigration documents
- tax returns (if relevant)

Veyco may perform:

- consistency checks
- data extraction
- formatting or metadata analysis
- fraud-risk scoring
- matching documents to identity

These checks do **not** constitute authentication or legal verification of the documents.

Partners are responsible for deciding whether the information is sufficient.

3.7 Right to Rent Evidence Collection

Where required, Veyco may collect and record:

- images of passports
- visas or endorsements
- immigration status
- evidence uploads
- Share Code results

Veyco does **not**:

- validate immigration status independently;
- interpret immigration law;
- confirm whether a User has the right to rent;
- provide immigration advice.

The Partner retains **full legal responsibility** for complying with the Immigration Act 2014 and related guidance.

3.8 Accuracy and Reliance

Identity Verification and biometric outputs:

- are based on automated checks + human factors,
- may contain errors,
- are influenced by the quality of data submitted, and
- may rely on third-party tools Veyco does not control.

Partners must not rely solely on verification results where:

- legal obligations require additional checks;
- there are inconsistencies in documents;
- the situation is high risk;
- the User's behaviour raises concerns.

The Services are **support tools**, not compliance substitutes.

3.9 Fraud Prevention & Misuse Monitoring

Veyco may monitor:

- patterns indicating fraud or misuse
- duplicate account attempts
- stolen identity signals
- abnormal behaviour
- unusually high-risk devices
- tampering signatures

If Veyco identifies activity that may indicate fraud, it may:

- flag the activity to the Partner
- suspend the User's verification process

- request additional documents
- limit access to the Platform
- contact relevant authorities if legally required

3.10 No Guarantee of Identity or Authenticity

Veyco **does not represent, warrant or guarantee**:

- the authenticity of any identity document;
- the accuracy of any User-submitted data;
- the results of biometric comparisons;
- that a User will not commit fraud;
- that a User has the legal right to rent, work, reside or contract;
- that the User is suitable for a tenancy or agreement.

Partners must make their own judgements and seek professional advice where necessary.

3.11 Evidence Storage and Audit Trails

Veyco may store:

- images
- videos
- document scans
- metadata
- signature events
- timestamps
- IP addresses
- audit logs
- certificate information

for:

- fraud prevention
- audit compliance
- legal obligations
- evidence of identity verification
- maintaining integrity of the Platform

Retention periods follow:

- statutory obligations (Right to Rent, AML);
- fraud-prevention standards;
- contractual obligations;
- regulatory guidance.

3.12 Updates to Identity Verification Methods

Veyco may update, replace or enhance its verification tools by:

- adopting new biometric technologies
- introducing additional fraud detection methods
- modifying workflows
- changing third-party suppliers
- improving accuracy and reliability
- updating data models

These updates may occur without notice where necessary for:

- security
- compliance
- prevention of fraud
- technical maintenance
- service continuity

3.13 Partner Responsibilities (Identity Verification)

Partners are responsible for:

- deciding which verification steps are necessary;
- ensuring lawful basis to process User data;
- interpreting verification results;
- notifying Users about required checks;
- handling disputes or questions about tenancy decisions;
- complying with all relevant legal and regulatory requirements;
- verifying the accuracy of their own instructions.

3.14 User Responsibilities (Identity Verification)

Users must:

- provide accurate and truthful information;
- follow instructions for identity checks;
- upload clear, current and valid documents;
- not impersonate others or submit false data;
- cooperate with additional verification steps if requested.

Submitting forged or altered documents may result in:

- reporting to authorities
- rejection of tenancy applications
- Partner notification
- account suspension

3.15 No Professional or Legal Advice

Identity Verification Services do **not** constitute:

- legal advice
- immigration advice
- compliance sign-off
- suitability assessments

Partners are responsible for obtaining legal or compliance advice as needed.

3.16 Open Banking and Financial Data

Where Open Banking Services are enabled, financial data obtained via Open Banking is used solely for tenancy referencing and affordability support. Such data does not form part of identity verification, does not constitute a credit check, and does not create any obligation on Veyco to assess financial suitability or risk.

3A. Optional Home-Move Support Services

3A.1 Overview

Veyco may work with carefully selected third-party partners to provide optional home-move and utilities-related support services ("**Home-Move Support Services**"). These services may include assistance with:

- change-of-occupancy notifications,
- council tax or utilities registration,
- broadband, TV or telecoms arrangements,
- insurance introductions, and
- other move-related administrative tasks.

These services are supplementary and separate from Veyco's Identity Verification Services.

3A.2 Contact by Third-Party Service Providers

Where relevant to the provision of Home-Move Support Services, a trusted third-party provider may contact Users directly by telephone, SMS or email to offer assistance. Users may decline such services at any time.

3A.3 Optional Nature of Services

Home-Move Support Services are entirely optional. If a User chooses to engage with a third-party service provider, any resulting agreement will be between the User and that provider. Veyco is not responsible for:

- the performance or suitability of any third-party service;
- pricing or commercial decisions made by the third-party provider;
- the accuracy of information provided by third parties;
- outcomes of services arranged between the User and a provider.

3A.4 Commission Disclosure

Veyco may receive a referral fee or commission if a User chooses to take up optional services offered by a third-party home-move partner. This does not affect the price paid by the User.

3A.5 No Impact on Identity Verification Services

Home-Move Support Services do not form part of Veyco's Identity Verification or Biometric Processing Services. These optional services do not affect the interpretation or reliability of identity verification outputs, and Users remain subject only to the requirements described in Section 3 when completing verification flows.

SECTION 4 — ACCOUNT CREATION, ACCESS & SECURITY

4.1 Authorised Users

The Partner may designate individuals as "**Authorised Users**" who may:

- access the Partner Dashboard;
- initiate checks;
- view Reports and audit logs;
- download documents;
- manage integration settings;
- The Partner:
- is responsible for all actions taken by Authorised Users;
- must ensure Authorised Users comply with these Terms;
- must revoke access promptly when individuals leave the organisation.

4.2 Account Security

The Partner must:

- keep login credentials secure;
- implement strong access controls;
- use industry-standard password practices;
- enable multi-factor authentication where offered;
- restrict access to authorised personnel only.

The Partner must not:

- share credentials between users;
- allow third parties to access the Platform using Partner credentials;
- store credentials insecurely.

4.3 API Credentials

If the Partner uses the API, Veyco will issue:

- API keys,
- client IDs, or
- other integration credentials.

The Partner must:

- store API keys securely,
- not embed keys in public-facing code,
- rotate keys if compromise is suspected,
- Misuse of API keys (including overuse, circumvention or abuse) may result in suspension.

4.4 Responsibility for Actions Under the Account

The Partner is responsible for:

- all activities under its Partner Account;
- identity checks initiated using its API keys;
- referencing workflows triggered by its systems;
- documents uploaded or sent for signature;
- actions taken by its Authorised Users.

Veyco is not responsible for unauthorised access caused by the Partner's security failures.

4.5 Account Configuration

Veyco may provide settings within the Partner Dashboard to control:

- branding;
- workflow options;
- permitted checks;
- signature templates;
- permissions for Authorised Users;
- which third-party integrations are enabled.

The Partner is responsible for selecting the correct settings.

4.6 Prohibited Account Activities

The Partner must not:

- access or use unauthorised parts of the Platform;
- attempt to bypass authentication or verification steps;
- interfere with system integrity or security;
- run automated scraping or extraction tools;
- simulate or test attacks (e.g., penetration testing) without prior written permission;

4.7 Account Suspension

Veyco may suspend the Partner Account (see Section 17) for:

- suspected fraud or misuse;
- suspected compromise of credentials;
- non-payment;
- legal or compliance issues;
- security threats;
- violation of these Terms.

Veyco will lift suspension once the underlying issue is resolved.

4.8 Account Termination

Upon termination of the Agreement:

- the Partner Account will be deactivated;
- API keys will be revoked;
- Authorised Users will lose access;
- data will be retained or deleted in accordance with Section 7.

SECTION 5 — QUALIFIED ELECTRONIC SIGNATURE – QES

5.1 Overview of Electronic Signature Services

Veyco provides electronic signature services that allow Users and Partners to electronically sign documents using:

- **Qualified Electronic Signatures (QES)**
- identity-verified signing flows
- digital certificates
- cryptographic validation
- audit trails
- timestamping
- secure evidence storage

QES processes are designed to meet the requirements of:

- the **Electronic Communications Act 2000**, and
- the **retained UK eIDAS Regulation**.

QES is the most secure and legally recognised form of electronic signature under UK law.

5.2 How QES Works

A Qualified Electronic Signature requires:

1. **Identity Verification**
   The signer completes identity verification (Section 3). This creates an identity assurance level suitable for QES.
2. **Signature Intent Confirmation**
   The signer views the document and confirms their intention to sign electronically.
3. **Cryptographic Signature Creation**
   A QES is created using cryptographic keys and a digital certificate.
4. **Certificate Generation**
   A Signature Certificate is issued, containing:
   - signer identity details
   - verification method
   - timestamps
   - certificate serial number
   - hash of the signed document
   - issuer information
5. **Signature Binding**

The certificate is cryptographically bound to the document.

6. **Audit Trail Completion**
   Veyco generates an Audit Trail showing:
   - document viewed
   - actions taken
   - device information
   - IP address
   - timestamps
   - verification results

This provides robust evidence for legal and compliance purposes.

5.3 Legal Effect of QES

A QES created through Veyco is intended to have the **same legal effect as a handwritten signature**, subject to UK law.

By using the Electronic Signature Services, Users and Partners agree that:

- QES may be relied on as evidence of signature
- signature certificates are binding
- audit trails may be used as evidence
- electronically signed documents are enforceable

This applies **to the fullest extent permitted by Applicable Law**.

5.4 Veyco Not a Party to Signed Documents

Unless explicitly agreed in writing:

- Veyco is **not a party** to any contract executed using the Platform
- Veyco is **not responsible** for the content, legality, validity, completeness or suitability of uploaded documents
- Veyco does **not** give legal advice regarding the documents
- Veyco does **not** verify whether signatories have the legal capacity or authority to sign

Partners are solely responsible for:

- preparing their own agreements
- ensuring documents are legally compliant
- ensuring the correct persons sign
- verifying authority where relevant (e.g., company signatories, guarantors)

5.5 User Responsibilities During Signing

Users must:

- read documents before signing
- ensure their information is correct
- not share signing links with others
- complete identity verification truthfully
- keep their devices secure
- notify Partners if errors or concerns arise

Signatures created using the User's device and identity verification may be treated as **their own** signature.

5.6 Partner Responsibilities for Uploaded Documents

If Partners upload documents for Users to sign, Partners must ensure:

1. **Content accuracy:**
   The document is correct, up to date and suitable for the intended purpose.
2. **Legality:**
   The document complies with:
   - tenancy law
   - consumer law
   - business law
   - contract law
   - specific statutory requirements (if any)
3. **Suitability:**
   The form, content and structure are appropriate for electronic signing.
4. **Signature order:**
   The correct parties are arranged in the correct sequence for signature.
5. **Identity of signatories:**
   The Partner selects the correct User(s) to sign the document.

6. **Retention:**
   Partners must store signed documents as required by their own internal policies.

Veyco **does not** audit or review documents uploaded by Partners.

5.7 Audit Trails

When a document is signed:

Veyco generates a comprehensive **Audit Trail**, which may include:

- document ID
- signer identity verification data
- email or mobile information
- device information
- IP address
- timestamps
- signature events
- certificate data
- hash values of documents
- version history

Audit Trails help Partners to demonstrate:

- the process used,
- authenticity of the signing event,
- and legal enforceability of the signature.

Audit Trails may be retained to comply with:

- contract law
- fraud prevention
- evidence requirements
- legal obligations
- operational integrity

5.8 Certificate Authority & Cryptographic Infrastructure

Veyco may use:

- in-house certificate infrastructure
- trusted third-party Certificate Authorities (CAs)
- cryptographic key generation
- time-stamping authorities
- qualified trust service providers

to generate and manage Signature Certificates.

The specific CA used may change from time to time for:

- security
- compliance with trust service requirements
- improved reliability

Details will appear in the Signature Certificate.

5.9 Document Integrity and Tamper Proofing

To preserve integrity:

- documents are hashed
- signatures are cryptographically bound
- the signed file is sealed
- any modifications invalidate the signature

If a signed document is altered after signing:

- the certificate will fail validation
- the Partner may be alerted
- the signed version stored by Veyco will remain original

5.10 Multi-Signature Workflows

Veyco supports:

- sequential signature flows
- parallel signature flows
- countersignatures
- multi-party agreements
- witness signatures (if applicable)

Partners configure:

- who signs
- in what order
- whether verification is required for each signer

Each signature event receives:

- its own certificate
- its own audit log
- its own timestamp

5.11 QES Limitations

While QES is the highest standard of electronic signature, Veyco cannot guarantee:

- enforceability of a specific contract
- suitability of documents for QES
- that all parties have the legal capacity to sign
- admissibility of evidence in any specific jurisdiction
- compatibility with certain specialist legal processes (e.g., wills, some deeds)

Some documents may **not** be eligible for electronic signing under UK law.
Partners must check this before using Veyco's Services.

5.12 Partner Responsibilities in Electronic Signing

Partners must:

- ensure documents are legally eligible to be electronically signed
- review the content for accuracy
- confirm whether witnessing is required
- ensure Users understand what they are signing
- verify that parties have legal authority
- ensure compliance with tenancy and contract law
- retain copies for their records

Veyco does **not** check these matters.

5.13 User Responsibilities in Electronic Signing

Users must:

- ensure they understand the document
- comply with their legal obligations
- sign only on their own behalf unless authorised
- not attempt to impersonate others
- maintain device and account security

5.14 Evidence Storage & Retrieval of Signed Documents

Veyco may store:

- signed documents
- certificates
- audit logs
- hashes
- metadata
- supporting evidence

Retention periods vary depending on:

- legal obligations
- fraud prevention requirements
- Partner contractual needs
- operational necessity

Partners may download signed documents for their own record-keeping.

5.15 Changes to QES Services

Veyco may modify QES Services to:

- improve security
- comply with changes in eIDAS or UK law
- adopt better cryptographic methods
- change certificate providers
- introduce additional safeguards
- remove outdated signing methods

Changes necessary for security or compliance may be introduced without prior notice.

SECTION 6 — API LICENCE & INTEGRATION TERMS

6.1 Overview of API Access

Where the Partner is provided with access to Veyco's API, these API Licence Terms apply in addition to the rest of the Terms.

API access enables Partners to:

- trigger identity verification flows
- initiate tenancy referencing applications
- embed verification or signing journeys in their own systems
- retrieve Reports and verification outcomes
- receive webhook updates
- automate workflows
- manage Users programmatically

Use of the API is a **privilege**, not a right, and may be withdrawn in accordance with these Terms.

6.2 Grant of Licence

Subject to these Terms, Veyco grants the Partner a:

- **non-exclusive**,
- **non-transferable**,
- **revocable**,
- **non-sublicensable**,

licence to use the API **solely** for the Partner's internal business purposes to access and use the Services.

Notwithstanding the above:

The Partner may allow authorised staff, contractors or integrated systems to use the API on its behalf, provided that:

- they act only on behalf of the Partner;
- they comply with these Terms;
- the Partner remains fully responsible for their actions.

6.3 API Keys and Authentication

API access requires an **API key**, which acts as a credential linked to the Partner's Account.

Partners must:

- keep API keys **confidential**;
- restrict API keys to necessary systems;
- rotate keys if compromise is suspected;
- implement secure storage practices;
- ensure only authorised personnel or systems use API keys.

Partners must immediately notify Veyco if an API key:

- is lost,
- is compromised,
- has been misused, or
- has been exposed publicly (e.g., GitHub, logs, shared code).

Veyco may temporarily disable keys to protect system security.

6.4 Permitted Uses

Partners may use the API for:

- **Identity verification**
  Initiating verification sessions for Users.
- **Tenancy referencing**
  Creating referencing applications via API endpoints.
- **Retrieving Reports**
  Pulling verification, referencing or signing outcomes.
- **Document upload**
  Where supported, uploading documents directly.
- **Electronic signature workflows**
  Initiating QES signing sessions programmatically.
- **Webhooks**
  Receiving status updates for automation.
- **Monitoring and audit**
  Confirming application status, errors, or outcomes.

Partners may only access **data related to Users they are legally entitled to process**.

6.5 Prohibited Uses

The Partner must **not**, and must ensure that no third party shall:

6.5.1 Data misuse

- use the API to harvest or scrape data
- use the API to build a competing product
- resell or redistribute Veyco's data
- use data to create consumer databases
- use data to screen people for unrelated purposes

6.5.2 AI and Machine Learning Restrictions

Partners must NOT:

- use ANY Veyco data (including images, documents, biometrics, metadata, reports, logs, or outcomes) to train, test, benchmark, validate or improve **any AI or machine-learning models**, including:
    - generative AI
    - facial recognition systems
    - identity models
    - classification systems
    - anomaly detection models
- upload data obtained from Veyco into any AI/ML training pipeline
- provide Veyco outputs to third parties for AI model development
- allow employees or vendors to use Veyco data in model R&D activities

This is a **strict and material condition** of the API licence.

6.5.3 Reverse Engineering

Partners must not:

- reverse engineer, decompile or disassemble the API
- attempt to discover source code
- bypass or modify security restrictions

6.5.4 Circumvention

Partners must not:

- circumvent rate limits
- interfere with API operations
- artificially inflate traffic
- create fake or automated Users
- use bots to trigger high-volume verification

6.5.5 Competitive Benchmarking

Partners must not:

- benchmark Veyco
- compare Veyco performance to competitors
- publish performance data
- conduct penetration tests without prior permission

6.5.6 Unlawful or Discriminatory Use

The API must not be used to:

- discriminate unlawfully against Users
- perform prohibited checks
- make decisions that violate housing or tenancy law
- conduct unauthorised immigration assessments

6.6 Rate Limits and Fair Use

Veyco may impose:

- rate limits,
- concurrency limits,
- throttle controls,
- volume caps, or
- other restrictions

to protect system performance and availability.

Partners must comply with these limits.

Veyco may adjust limits from time to time:

- to maintain system health,
- to prevent abuse, or
- to ensure fair usage across customers.

6.7 Security Requirements

Partners must:

- implement industry-standard security measures
- use HTTPS or equivalent secure transport
- secure API keys with secret management tools
- prevent client-side exposure of credentials
- use firewalls, access controls and logging
- encrypt sensitive data
- store minimal personal data locally

Partners must not embed API keys in:

- mobile apps,
- client-side JavaScript,
- public repositories,
- demo environments, or
- unsecured code.

6.8 API Changes and Versioning

Veyco may:

- release new API versions
- deprecate old endpoints
- modify parameters or response formats
- introduce new authentication methods
- update documentation

Changes may occur:

- for security
- for compliance
- to improve functionality
- due to third-party provider changes

Veyco will provide reasonable notice of breaking changes wherever practicable.

6.9 Suspension or Termination of API Access

Veyco may suspend or terminate API access if:

- the Partner breaches these Terms
- the Partner misuses data
- API keys are compromised
- activity threatens system security
- illegal or fraudulent activity is detected
- requests exceed fair-use limits
- payments are overdue
- compliance obligations require it

Suspension may occur without notice where necessary to protect:

- system integrity
- other Users
- legal or regulatory compliance

6.10 Data Protection in API Use

When using the API:

- the Partner is **Controller** for User data they request
- Veyco acts as **Processor** for processing on the Partner's instructions
- both parties must comply with Data Protection Laws
- secure transfer of data through the API is the Partner's responsibility

Partners must:

- ensure a lawful basis for each use of the API
- use data only for permitted purposes
- delete data when no longer necessary
- provide privacy information to Users

API logs may be retained for:

- fraud prevention
- security
- audit and evidence
- compliance
- dispute resolution

6.11 Integration Support

Veyco may provide:

- API documentation
- SDKs (if available)
- sample requests
- integration guidance
- technical support
- webhook troubleshooting

Veyco is not responsible for:

- the Partner's internal systems
- failures in third-party platforms
- losses arising from integration errors
- misconfigured webhooks or endpoints
- downtime caused by the Partner's infrastructure

6.12 Liability for API Use

Partners are liable for:

- all activities conducted via their API keys
- any misuse of the API
- unlawful instructions
- automated misuse (including bots or scripts)
- breaches caused by insecure systems
- third parties using API keys issued to them

Veyco is **not** responsible for:

- lost data due to improper integration
- incorrect use of endpoints
- errors caused by Partner infrastructure
- decisions made based on API outputs

6.13 End of API Licence

The API licence ends:

- when the Partner's agreement with Veyco ends,
- when Veyco terminates API access under these Terms, or
- when the Partner ceases using the Services.

Upon termination:

- API access stops immediately
- API keys must be deleted
- the Partner must stop using all API data except for records they are legally entitled to retain
- Partner systems must remove Veyco integrations

SECTION 7 — DATA PROTECTION & PRIVACY

7.1 Overview and Compliance

Both Veyco and the Partner agree to comply with all **Data Protection Laws**, including:

- UK General Data Protection Regulation ("UK GDPR")
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- any binding guidance or codes issued by the ICO

This section explains how Personal Data is handled when:

- Identity Verification Services are used
- Tenancy Referencing Services are used
- Electronic Signature (QES) workflows are used
- APIs are used
- Reports are generated
- Audit Trails are created

7.2 Roles of the Parties (Controller / Processor Model)

7.2.1 Partner as Controller; Veyco as Processor

For the majority of processing activities carried out when delivering the Services:

- The **Partner** acts as the **Controller**.
- **Veyco** acts as a **Processor**, acting only on the Partner's lawful instructions.

This includes processing:

- identity data uploaded by Users
- referencing information
- documents (e.g., payslips, bank statements)
- identity verification outputs
- signing flows initiated by the Partner
- reports generated for the Partner
- data submitted via the API

The Partner is responsible for:

- having a lawful basis (Article 6 UK GDPR)
- meeting transparency obligations
- ensuring data minimisation
- complying with Right to Rent, AML or other legal duties
- responding to User data subject requests

7.2.2 Veyco as Independent Controller

Veyco acts as an **Independent Controller** for processing relating to:

- fraud prevention
- security monitoring
- detecting suspicious or malicious activity
- platform integrity
- audit logs necessary for platform protection
- compliance with legal obligations (e.g., statutory Right to Rent retention)
- internal record keeping for legal defence

7.2.3 Joint Controller Situations

Certain processes may involve **Joint Controllership**, including:

- production of Right to Rent evidence where both parties determine purposes
- certain fraud-detection workflows
- evidence retention required by law

In these cases:

- the Partner and Veyco agree to allocate responsibilities fairly
- Veyco will handle system-level obligations
- the Partner handles tenancy decision obligations

7.2.4 Open Banking Data

In relation to Open Banking Services:

- the Partner acts as Controller of all Open Banking data obtained for tenancy referencing and affordability assessment purposes;
- Veyco acts as Processor, processing such Open Banking data solely on the Partner's documented instructions and in accordance with this Agreement; and
- FCA-authorised Open Banking providers and AISPs act as independent controllers and/or processors in accordance with their own regulatory obligations, privacy notices and contractual arrangements.

Veyco does not receive, store or have access to User banking credentials and does not access User payment accounts other than through the Open Banking framework operated by authorised third-party providers.

7.3 Lawful Bases for Processing

Depending on the activity, processing may rely on:

7.3.1 Contract

To deliver the Services requested by the Partner and the User.

7.3.2 Legitimate Interests

For purposes including:

- fraud detection
- platform security
- audit and logging
- analysis for service improvement
- customer support
- prevention of misuse

A balancing test ensures interests do not override User rights.

7.3.3 Legal Obligation

For example:

- Right to Rent evidence
- record-keeping for law enforcement
- fraud and AML-related retention (where applicable)
- responding to lawful requests from authorities

7.3.4 Explicit Consent (Biometrics)

Where required for:

- facial biometric comparison
- liveness detection
- capturing biometric templates

Consent is:

- freely given
- informed
- unambiguous
- recorded electronically

7.3.5 Substantial Public Interest (Data Protection Act 2018)

For:

- identity verification
- fraud prevention
- Right to Rent evidence
- preventing unlawful acts

7.4 Categories of Personal Data Processed

Veyco may process:

7.4.1 Identity Data

- full name
- address(es)
- date of birth
- contact details
- nationality (if provided)
- identity documents

7.4.2 Biometric Data (Special Category)

- facial images
- liveness detection data
- biometric vectors used for comparison

7.4.3 Referencing Information

- employment & income data
- payslips and financial documents
- guarantor details
- landlord references
- tenancy information

7.4.4 Document Data

- passports, driving licences
- bank statements
- proof of address
- tenancy agreements
- supporting documents

7.4.5 Device & Technical Data

- IP address
- device fingerprint
- browser and OS
- fraud prevention metadata
- timestamps

7.4.6 Electronic Signature Data

- signature intent
- audit logs
- certificates
- signer identity data
- cryptographic evidence
- document hashes

7.4.7 Customer Support Data

- communications
- logs
- screenshots or recordings (if voluntarily supplied)

7.5 Instructions From the Partner

Veyco will:

- act only on the Partner's documented instructions
- process data only to deliver the Services
- not use data for purposes unrelated to the Services
- notify the Partner if an instruction breaches Data Protection Laws
- ensure staff confidentiality
- implement security measures (see Section 7.8)

If a Partner gives an unlawful instruction (knowingly or unknowingly), Veyco may suspend processing and clarify the request.

7.6 Sub-Processing

Veyco may use **Sub-Processors** to deliver the Services, including:

- identity verification providers
- biometric engines
- document analysis tools
- fraud-prevention systems
- cloud hosting providers
- email or notification services
- trust service providers (for QES)

Veyco ensures that all Sub-Processors:

- are bound by written contracts
- implement adequate security
- comply with equivalent data protection obligations

The Partner authorises Veyco to appoint Sub-Processors as reasonably necessary.

A current list may be included in the Privacy Policy or on the Veyco website.

7.7 International Transfers

Where Personal Data is transferred outside the UK, Veyco will ensure:

- appropriate safeguards
- International Data Transfer Agreements (IDTAs)
- Standard Contractual Clauses (if required)
- supplementary measures (security and encryption)

Transfers will occur only where lawful and necessary.

7.8 Security Measures

Veyco implements technical and organisational measures including:

- encryption in transit and at rest
- secure storage of audit logs
- strict access controls
- role-based access
- multi-factor authentication
- network monitoring
- segmentation of sensitive data
- vulnerability scanning
- incident response procedures

Partners are responsible for:

- securing their own systems
- securing API keys
- staff training
- controlling access to the Partner Dashboard

7.9 Data Subject Rights

Users have rights under UK GDPR, including the right to:

- access
- rectification
- erasure (in certain cases)
- restriction
- objection
- data portability
- withdraw consent (where applicable)

Users may submit requests to: compliance@veyco.com

Veyco will:

- respond within statutory timeframes
- assist the Partner in responding to User requests
- inform the Partner of requests relating to processing done on its behalf

7.10 Data Breaches

If Veyco becomes aware of a **Personal Data Breach** affecting Partner data, Veyco will:

- notify the Partner without undue delay
- provide known details
- cooperate with investigations
- assist the Partner in meeting any legal obligations

The Partner is responsible for reporting breaches to:

- the ICO (if required)
- affected individuals (if required)

Veyco will maintain breach logs and follow internal response procedures.

7.11 Retention and Deletion

Personal Data is retained for:

- the duration necessary to deliver the Services
- legal retention obligations (e.g., Right to Rent)
- fraud prevention
- defending legal claims
- audit requirements

Typical retention periods may include:

- identity verification data: 12–36 months
- signed documents: duration of tenancy + retention period
- Right to Rent evidence: statutory retention (e.g., one year after tenancy ends)
- audit logs: up to 7 years, for legal defence

Upon termination:

- data is either deleted or pseudonymised
- backups are purged according to their lifecycle

Partners may request earlier deletion, but Veyco may retain data where required by law or for fraud prevention.

7.12 Data Portability & Export

Veyco may allow Partners to export:

- Reports
- signed documents
- audit trails
- raw referencing data
- Right to Rent evidence

Formats may include:

- PDF
- machine-readable JSON (API)

7.13 Partner Responsibilities

Partners are responsible for:

- ensuring lawful basis for processing
- providing privacy notices to Users
- obtaining necessary consents (where applicable)
- ensuring accuracy of information they enter
- ensuring they comply with Right to Rent laws
- responding to user enquiries
- conducting tenancy decisions in a lawful manner
- securing data on their own systems

Partners must not use the Services in ways that violate:

- data protection laws
- discrimination laws
- consumer protection laws
- landlord and tenant laws

7.14 Automated Decision-Making

Veyco does **not** carry out automated decision-making that produces legal or similarly significant effects.

Verification scores and risk indicators are **support tools only**.

Partners must make **final decisions** themselves.

7.15 Marketing Communications

Veyco may:

- send service-related messages
- send account updates
- notify of security issues
- provide system alerts

Marketing emails require **consent** or a **soft opt-in** where allowed.
Users may opt out at any time.

7.16 Records of Processing

Veyco maintains:

- records of processing activities
- data flow maps
- data protection impact assessments (where required)
- security documentation
- processor/sub-processor agreements

Partners must maintain their own records as Controllers.

7.17 Privacy Policy

Veyco maintains a **separate Privacy Policy**, which:

- describes in detail how data is processed
- supplements this section
- is accessible on the Veyco website
- forms part of these Terms

If there is a conflict, the Terms prevail except where the Privacy Policy is legally required to take precedence.

SECTION 8 — AVAILABILITY, MAINTENANCE & SERVICE LEVELS

8.1 General Availability

Veyco aims to ensure the Platform and Services are available **24 hours per day, 7 days per week**, except during planned or emergency maintenance.

However, the Partner acknowledges that:

- availability depends partly on third-party services;
- downtime may occur due to circumstances outside Veyco's control;
- no online service can guarantee 100% uptime;
- Veyco does not warrant uninterrupted or error-free operation of the Services.

Veyco will use reasonable efforts to:

- maintain reliable uptime;
- monitor performance;
- respond to incidents quickly;
- minimise disruption to Users and Partners.

8.2 Planned Maintenance

Veyco may perform planned maintenance to:

- upgrade infrastructure;
- apply patches;
- deploy new features;
- replace or repair hardware;
- update software dependencies.

Where practicable:

- Veyco will schedule maintenance outside of business-critical hours;
- advance notice of significant maintenance will be provided to Partners.

Minor or non-impacting updates may be deployed without notice.

8.3 Emergency Maintenance

Veyco may perform emergency maintenance when necessary to:

- fix security vulnerabilities;
- address service degradation;
- prevent data loss or corruption;
- respond to third-party outages;
- maintain operational integrity.

Emergency maintenance may be carried out **without prior notice**.

8.4 Third-Party Dependencies

The Services rely on external providers including:

- identity verification engines;
- biometric analysis tools;
- document scanning providers;
- email and SMS delivery systems;
- hosting infrastructure;
- certificate authorities;
- open-data sources;
- fraud-prevention tools.

Veyco does not guarantee the continued availability or performance of third-party systems.

However, Veyco will:

- select reputable providers;
- monitor service health;
- switch or re-route providers when necessary;
- protect against cascading failures.

8.5 Support Services

Veyco provides support to Partners via:

- email: **support@veyco.com**
- in-platform messaging (meta whatsapp)
- technical support channels (for API customers)

Support includes:

- troubleshooting service issues;
- guidance on correct use of the Platform;
- help interpreting error messages;
- investigation of unexpected results;

Support availability may be:

- standard business hours (UK-based), or
- enhanced availability where a Premium SLA is agreed in writing.

8.6 Incident Reporting

Partners should promptly report:

- service issues;
- unexpected downtime;
- verification errors;
- referencing inaccuracies;
- signing issues;
- API outages or errors;
- security concerns.

Veyco will:

- log incidents;
- triage severity;
- take reasonable steps to resolve issues;
- provide updates where appropriate.

8.7 No Guarantee of Perfect Performance

While Veyco strives for high reliability, the Partner acknowledges that:

- delays may occur;
- verification may require retries;
- document scanning may fail;
- biometrics may require re-capture;
- email or SMS delivery may be delayed or blocked;
- API responses may occasionally fail or time out.

These issues do not constitute a breach unless part of a specific written SLA.

8.8 Updates and Improvements

Veyco may update:

- verification methods;
- referencing workflows;
- signing flows;
- API versions;
- dashboards and UI elements.

Updates are intended to:

- improve security;
- enhance performance;
- meet regulatory requirements;
- respond to industry changes;
- add new features;
- fix bugs or vulnerabilities.

Veyco may deploy updates without Partner approval.

8.9 Discontinuation of Features

Veyco may discontinue or replace certain features where necessary, including:

- outdated verification methods;
- redundant APIs;
- legacy identity-checking suppliers;
- functionality no longer supported by third parties.

Veyco will:

- give reasonable notice of major deprecations where possible;
- offer migration paths when feasible;
- minimise disruption to the Partner.

8.10 No Liability for Third-Party Outages

Veyco is not responsible for:

- outages of identity verification vendors;
- downtime of certificate authorities;
- interruptions to biometric engines;
- telecoms failures;
- SMS gateway failures;
- cloud hosting outages;
- internet or network failures beyond Veyco's control.

Veyco will act reasonably to mitigate disruptions but does not accept liability for events beyond its reasonable control.

8.11 Service Suspension

Veyco may temporarily suspend access to the Services where:

- required for maintenance;
- necessary for security;
- misuse or suspicious activity is detected;
- non-payment occurs;
- a legal or regulatory request requires suspension;
- system overload or attack makes suspension necessary.

Suspension will be for the minimum time required to address the issue.

8.12 Partner System Requirements

Partners must ensure:

- a stable internet connection;
- supported browser versions;
- reasonable system performance;
- correct integration for API use;
- secure networks and devices;
- no blocking of essential domains or ports.

Veyco is not responsible for:

- issues caused by the Partner's IT infrastructure;
- use of unsupported browsers;
- firewall restrictions;
- outdated systems.

SECTION 9 — REPORTS, RESULTS & RELIANCE

9.1 Nature of Reports

Veyco generates various Reports and outputs ("Reports") as part of:

- identity verification,
- biometric checks,
- document analysis,
- tenancy referencing, and
- electronic signature workflows.

Reports may include:

- pass/fail outcomes
- verification summaries
- extracted data
- biometric confidence scores
- liveness detection outcomes
- document consistency checks
- tenancy referencing assessments
- affordability calculations
- fraud-risk indicators
- signature certificates
- Right to Rent evidence summaries

Reports are provided **for information purposes only**.

9.2 Reports Do Not Constitute Advice

Reports **are not**:

- legal advice,
- immigration advice,
- risk assessments,
- tenancy approval or rejection recommendations,
- advice on creditworthiness,
- financial advice, or
- compliance certification.

Veyco does **not** advise on:

- whether a User should be accepted as a tenant;
- whether a User meets affordability requirements;
- whether a User is compliant with immigration rules;
- whether a User will pay rent or follow a tenancy;
- or whether documents submitted by Users are genuine.

Partners must **not** construe Reports as being authoritative or determinative.

9.3 Limitations of Reports

Reports may be affected by:

- the quality of User-provided images;
- accuracy of third-party databases;
- document tampering undetectable by automated tools;
- limitations of biometric technology;
- fraudulent attempts designed to evade detection;
- employer or landlord misrepresentation;
- errors in manual data extraction;
- inconsistencies in supporting evidence.

Veyco does not guarantee:

- accuracy of all extracted data,
- detection of all fraudulent documents,
- correctness of referencing assessments,
- availability of third-party verification engines.

9.4 Reliance and Partner Responsibilities

Partners agree and acknowledge that:

1. **Final responsibility remains with the Partner.**
   Reports assist decision-making but **do not replace Partner judgement**.
2. **Reports are one input among many.**
   Partners must consider additional factors such as:
   - User-supplied information
   - tenancy history
   - affordability policies
   - in-person assessments
   - legal obligations
   - contextual facts
3. **Reports do not override regulatory duties.**
   This includes duties under:
   - Right to Rent
   - consumer protection law
   - discrimination law
   - tenancy law
   - AML or fraud rules
   - landlord obligations
4. **Reports may contain limitations.**
   Partners must interpret findings responsibly.
5. **Reports are not binding.**
   Veyco does not instruct Partners to accept or reject a User.

9.5 No Guarantee or Warranty

Veyco does **not** guarantee that:

- identity documents are valid,
- the User is who they claim to be,
- liveness detection is always accurate,
- referenced affordability levels are correct,
- referencing conclusions are complete,
- signed documents are enforceable,

- data from external sources is reliable.

Reports do not guarantee outcomes, suitability or compliance.

9.6 Right to Correct Errors

If the Partner or User identifies an error in a Report:

- Veyco will review the issue;
- Veyco may request additional evidence;
- Veyco may update or amend the Report;
- Veyco may re-run verification where appropriate;
- Veyco is not responsible for errors in User-provided information.

Corrections may not be possible if:

- documents have expired,
- verification tools require new captures,
- the original data has been overwritten or deleted due to retention limits.

9.7 Access to Reports

Reports are made available via:

- the Partner Dashboard;
- email notification (where applicable);
- secure download links;
- API endpoints;
- webhook notifications.

Partners must:

- store Reports securely,
- ensure only authorised personnel access them,
- not share Reports improperly,
- comply with Data Protection Laws.

9.8 Use of Reports

Partners may use Reports for:

- tenancy decision-making;
- compliance with legal obligations;
- assessing identity validity;
- referencing applications;
- QES audit and evidence;
- fraud prevention;
- resolving disputes with Users.

Partners must **not**:

- use Reports for unrelated purposes,
- use Reports to train AI or machine-learning models,
- resell or redistribute data from Reports,
- rely solely on Reports for critical decisions without human oversight.

Any misuse constitutes a **material breach** of these Terms.

9.9 Report Storage and Retrieval

Veyco may store Reports for:

- Partner access,
- audit trails,
- compliance obligations,
- legal defence,
- fraud detection,
- platform integrity.

Retention periods depend on:

- the nature of the Report,
- statutory retention requirements,
- fraud-prevention obligations,
- operational need.

Veyco will delete Reports in accordance with Section 7 (Data Protection & Privacy).

9.10 Third-Party Data

Some Report content may originate from:

- government sources,
- public databases,
- identity checking providers,
- sanctions lists,
- email or telephone verification systems,
- document validation systems.

Veyco does not control the accuracy of third-party data.

Partners must verify critical information independently.

9.11 Changes to Report Formats

Veyco may update the layout, content, structure or format of Reports to:

- improve clarity,
- include additional checks,
- comply with regulatory changes,
- enhance fraud detection,
- add new data fields.

Veyco will provide reasonable notice of significant Report format changes.

SECTION 10 — AUDIT TRAILS & EVIDENCE FILES

10.1 Overview of Audit Trails

Veyco generates **Audit Trails** as part of identity verification, referencing, fraud-prevention and electronic signing processes. These serve as a **chronological record of events**, providing evidence that:

- the User participated in the process,
- the correct steps were followed,
- identity or signing events occurred in sequence,
- fraud-prevention checks were performed, and
- the resulting Reports or signed documents are valid.

Audit Trails may form part of the legal and evidential integrity of the Services.

10.2 What Audit Trails Contain

Depending on the Service, an Audit Trail may include some or all of:

10.2.1 User Actions

- session creation
- verification started
- document upload
- biometric capture
- referencing data submitted
- signature intent displayed
- signature performed

10.2.2 Technical Metadata

- IP address
- geolocation (approximate, based on IP)
- device fingerprint or ID
- operating system and browser
- timestamp of each step
- identity verification provider used
- signature certificate details
- audit hashes of documents

10.2.3 Document & Data Capture

- document scans
- extracted data
- version history of document captures
- internal processing results
- fraud indicators or flags

10.2.4 Signature Evidence (QES)

- signer identity information
- certificate authority details
- cryptographic seal
- integrity validation proofs
- document hash pre- and post-signing
- QR code or verification link (if applicable)

10.2.5 Referencing Evidence

- employment documents submitted
- affordability calculations
- supporting evidence metadata
- exception or anomaly indicators

Audit Trails are generated **automatically** to ensure completeness, reliability and standardisation.

10.3 Purpose of Audit Trails

Audit Trails are maintained to:

- demonstrate identity verification steps occurred;
- support the validity of electronic signatures;
- satisfy legal and regulatory obligations (including eIDAS and Right to Rent);
- detect fraud;
- assist in resolving disputes;
- maintain platform integrity;
- provide Partners with evidence of checks performed;
- respond to legal or regulatory requests;
- provide an authoritative record of signing events.

Audit Trails protect **both Partners and Users**.

10.4 Storage of Audit Trails

Audit Trails, Signature Certificates and supporting evidence may be stored:

- in encrypted storage,
- with restricted access controls,
- subject to secure backups,
- within environments designed for evidential integrity.

Storage locations may include cloud infrastructure based in:

- the UK
- the EEA
- other jurisdictions with appropriate safeguards (e.g., using IDTAs or SCCs)

All storage complies with Data Protection Laws (see Section 7).

10.5 Access to Audit Trails

Access to Audit Trails is controlled as follows:

10.5.1 Partner Access

Partners may:

- retain copies in their internal systems

Partners must not:

- share Audit Trails with unauthorised persons
- use Audit Trails for unrelated purposes
- upload Audit Trails to systems lacking adequate security

10.5.2 User Access

Upon request, Users may:

- request access to certain audit data that relates to them
- request copies of signed documents
- request confirmation of verification steps

Some internal fraud signals or proprietary logs may not be disclosed for security reasons.

10.5.3 Veyco Internal Access

Internal access is:

- controlled
- logged
- role-based
- limited to operational and support staff on a need-to-know basis

10.6 Audit Trails for Electronic Signatures (QES)

QES Audit Trails are especially important for:

- demonstrating signer identity
- proving integrity of the signed document
- reconstructing the signing process
- verifying certificate authenticity
- showing sequence of signature events
- resolving disputes regarding signature validity

Electronic Signature Audit Trails may include:

- intent confirmation (e.g., “Click to sign”)
- pre-sign view of document
- signing timestamp
- device and session identifiers
- certificate details
- cryptographic binding information
- evidence of document integrity before and after signing

These may be admissible as evidence in court or arbitration.

10.7 Right to Rent Evidence Logs

Where the Services are used to support Right to Rent processes, Veyco may record:

- Share Code search results
- Home Office response data
- identity document images
- timestamps showing when the check was performed
- metadata confirming the check was valid at that time

These logs help Partners demonstrate compliance with statutory duties.

10.8 Fraud-Prevention Audit Trails

Fraud-prevention logs may contain:

- device anomalies
- behavioural patterns
- high-risk indicators
- account correlation signals
- multiple failed verification attempts
- suspicious document metadata

These logs:

- are retained for fraud prevention,
- may be shared with authorities where legally required,
- may influence future verification decisions.

10.9 Retention of Audit Trails

Audit Trails are retained for:

- compliance purposes
- legal obligations
- fraud prevention
- evidentiary purposes
- defending legal claims
- operational continuity

Retention periods may vary depending on:

- regulatory requirements (e.g., Right to Rent retention)
- fraud-prevention needs
- the nature of the signed document
- disputes or ongoing investigations

Typical retention windows:

- identity verification logs: 12–36 months
- QES evidence: duration of contract + retention period
- Right to Rent evidence: statutory retention period (e.g., one year after tenancy end)
- audit logs: up to 7 years (legal defence)

Veyco may retain pseudonymised or aggregated data indefinitely for anti-fraud training and analytics **unless prohibited** by law.

10.10 Deletion of Audit Trails

Upon request or termination:

- Veyco will delete or anonymise Audit Trails where possible
- unless required to retain them by law, regulations, fraud-prevention needs or legitimate interests
- backups are purged on their lifecycle schedule

Partners may request earlier deletion of specific records, but Veyco may refuse where:

- deletion undermines fraud prevention;
- legal obligations require retention;
- ongoing disputes necessitate evidence retention.

10.11 Modifications to Audit Trail Structure

Veyco may modify:

- the structure of Audit Trails
- data fields collected
- logging formats
- certificate metadata
- internal evidence standards

to:

- comply with regulatory changes
- improve fraud detection
- enhance evidence integrity
- respond to updated cryptography standards
- integrate new verification or signing engines

Significant changes will be communicated to Partners where reasonable.

SECTION 11 — INTELLECTUAL PROPERTY RIGHTS

11.1 Ownership of the Platform and Services

Veyco and/or its licensors own all Intellectual Property Rights in:

- the Platform;
- identity verification workflows;
- referencing workflows;
- electronic signature systems;
- QES certificates and cryptographic infrastructure;
- APIs and SDKs;
- analytics and fraud-detection tools;
- dashboards and UX/UI elements;
- templates, designs and layouts;
- system logic, algorithms and processes;
- all associated software, code, databases and content.

Nothing in these Terms transfers ownership of Veyco's Intellectual Property to the Partner.

The Partner receives **a licence**, not ownership.

11.2 Intellectual Property in Partner Content

"Partner Content" includes:

- tenancy agreements;
- reference request forms;
- User data provided to Veyco;
- employer or landlord details;
- instructions;
- any documents the Partner uploads.

The Partner retains all Intellectual Property Rights in Partner Content.

By uploading Partner Content, the Partner grants Veyco a:

- **non-exclusive**,
- **worldwide**,
- **royalty-free**,
- **transferable**,
- **sublicensable (to Sub-Processors)**,
- **fully paid-up**,

licence to use, reproduce, process, store, analyse and display Partner Content **solely for the purpose of providing the Services**.

Veyco will:

- not use Partner Content for marketing
- not resell Partner Content
- not use Partner Content to train general-purpose AI models
- not disclose Partner Content except as permitted under these Terms

11.3 Intellectual Property in User Content

"User Content" includes:

- identity documents
- biometric captures
- referencing information
- signature events
- documents signed by Users
- Right to Rent evidence
- uploaded files and supporting documents

Users retain all Intellectual Property Rights in their own content.

Veyco receives a licence to process User Content **as processor on the Partner's instructions**, or independently where required by law or for fraud prevention (Section 7).

11.4 Reports, Scores, Certificates & Audit Trails

All Reports, identity verification outputs, referencing assessments, signature certificates and audit trails:

- are generated by Veyco;
- contain elements of Veyco Intellectual Property;

- are licensed to the Partner for their internal business use only.

Partners may:

- store Reports;
- use them for tenancy-related, onboarding, compliance, verification, execution and risk-assessment purposes in connection with property-related transactions;
- retain them for legal compliance;
- share them with Users where appropriate.

Partners may **not**:

- sell Reports;
- resell Veyco outputs;
- publish system performance data;
- use Reports for model training;
- share Reports with competitors of Veyco;
- use Reports for purposes unrelated to the tenancy workflow.

11.5 Licence to Use the Platform

Veyco grants the Partner a:

- **non-exclusive**,
- **non-transferable**,
- **revocable**,
- **non-sublicensable**

licence to access and use the Platform during the Term, solely:

- for internal business use;
- for identity verification and referencing;
- for electronic signature workflows;
- for lawful tenancy-related purposes;
- in accordance with these Terms.

Any other use requires prior written permission from Veyco.

11.6 Licence to Use the API

If API access is provided, the API Licence in **Section 6** applies.

This section incorporates those restrictions by reference.

11.7 Restrictions on Use

Partners must **not**:

1. **copy, modify, adapt or create derivative works** of the Platform;
2. reverse engineer, decompile or disassemble the Platform;
3. remove or obscure copyright notices or branding;
4. access the Platform for the purpose of building a competing service;
5. allow unauthorised third parties to access the Platform;
6. attempt to circumvent security or authentication;
7. scrape or extract data outside normal usage;
8. benchmark performance unless expressly permitted;
9. use Veyco data for training AI or machine-learning models;
10. resell Veyco services without written permission.

These restrictions are material conditions of use.

11.8 No Transfer of Ownership

Nothing in these Terms:

- transfers any Intellectual Property Rights from Veyco to the Partner;
- grants the Partner exclusivity;
- allows the Partner to claim ownership or authorship of Veyco systems;
- creates any joint-development rights unless expressly agreed.

All rights not expressly granted are reserved by Veyco.

11.9 Feedback

If the Partner or its staff provide feedback, ideas, suggestions or proposals to Veyco (collectively, “Feedback”):

- Veyco may use the Feedback freely
- Veyco may incorporate Feedback into its products
- Veyco has no obligation to compensate the Partner
- Feedback does not create any joint-IP rights

Partners must only provide Feedback they have the right to share.

11.10 Branding, Marks & Logos

Veyco's:

- names,
- logos,
- trademarks,
- design marks, and
- domain names

are protected by Intellectual Property Laws.

Partners must **not**:

- use the Veyco name or logo without written permission;
- register similar or confusing names or domains;
- imply endorsement by Veyco.

Veyco may reference the Partner as a client **only if** permitted in writing.

11.11 Third-Party Intellectual Property

Certain components of the Services may:

- incorporate third-party copyrighted content;
- use open-source software;
- rely on licensed biometric or document analysis engines;
- use certificate authorities and QES providers.

Use of third-party components is subject to their respective terms.

Partners must comply with any flow-down obligations communicated to them.

11.12 Obligations on Partner Staff

The Partner must ensure that:

- all authorised users comply with these Intellectual Property restrictions;
- API keys and dashboard access credentials are secure;
- internal staff do not misuse Veyco content.

The Partner is responsible for actions taken by its staff, contractors or systems that it configures.

11.13 Survival

All Intellectual Property clauses continue after termination of:

- the Agreement;
- the Partner's access;
- use of the Platform or API.

The Partner must:

- stop using Veyco Intellectual Property
- delete API keys
- cease all use of Reports except where legally required to retain them

upon termination of the Agreement.

SECTION 12 — CONFIDENTIALITY

12.1 Definition of Confidential Information

"**Confidential Information**" means any information disclosed by one party ("**Disclosing Party**") to the other ("**Receiving Party**") whether verbally or in writing, that:

- is marked as confidential;
- is stated to be confidential; or
- would reasonably be understood to be confidential given the nature of the information or the circumstances of disclosure.

Confidential Information includes, without limitation:

12.1.1 Veyco Confidential Information

- the Platform, Services, and underlying technology;
- verification methods, algorithms, models, processes, workflows;
- pricing, commercial terms and contracts;
- API keys, documentation, credentials;
- system logs, monitoring data and security measures;
- internal policies, procedures, architecture and infrastructure;
- fraud-detection logic;
- all Intellectual Property in the Platform.

12.1.2 Partner Confidential Information

- tenancy agreements and templates;
- internal policies and procedures;
- pricing, commercial terms or procurement information;
- API usage details;
- business plans and strategies.

12.1.3 User Information

User information (Personal Data or otherwise) disclosed via the Services is treated as Confidential Information of the Partner and the User.

12.2 Exclusions

Confidential Information does **not** include information that:

1. **is or becomes public** other than through breach of this Agreement;
2. **was lawfully known** to the Receiving Party before disclosure;
3. **is lawfully received from a third party** without restriction;
4. **is independently developed** by the Receiving Party without using the Disclosing Party's information;
5. is required to be disclosed by **law, court order, regulator or government authority**, provided that the Receiving Party (where lawful) gives reasonable notice to the Disclosing Party.

12.3 Obligations of the Receiving Party

The Receiving Party must:

1. **keep Confidential Information secret**;
2. **use it only** to perform obligations or exercise rights under the Agreement;
3. **not disclose** it to third parties except as permitted;
4. **protect** it using at least the same degree of care used to protect its own confidential information (and no less than reasonable care);
5. take reasonable steps to ensure its employees, contractors and agents comply with these confidentiality obligations.

12.4 Permitted Disclosures

The Receiving Party may disclose Confidential Information to:

- employees, officers or contractors
- professional advisers (legal, accounting, compliance)
- Sub-Processors (in the case of Veyco)
- service providers assisting with the Services (subject to confidentiality safeguards)

provided that:

- each recipient has a **need to know**, and
- recipients are bound by confidentiality duties at least as strict as this Section.

12.5 Confidentiality of User Data

Both parties agree that:

- all Personal Data collected for identity verification, referencing, signatures or onboarding is confidential;
- detailed restrictions on Personal Data appear in **Section 7**;
- confidentiality obligations apply to both identified and pseudonymised data;
- audit trails, Reports, certificates and signature files are confidential.

Partners must not:

- share User data with third parties except where legally allowed;
- publish Reports or sensitive data;
- use User data for unrelated purposes;
- upload Veyco-provided User data into external systems without adequate security.

12.6 Protection of Veyco Security Information

The Partner must not disclose:

- security protocols;
- API rate limits;
- fraud-detection logic;
- platform architecture;
- vulnerability details;
- internal logs, code or algorithms.

Such information is sensitive Confidential Information of Veyco and protected to a higher standard.

12.7 Compelled Disclosure

If the Receiving Party is legally required to disclose Confidential Information:

- it must (where lawful) notify the Disclosing Party promptly;
- allow reasonable time for objections or protective measures;
- disclose only the minimum required to comply;
- continue treating the remainder as confidential.

12.8 Return or Destruction

Upon termination of the Agreement, or on request:

- the Receiving Party must delete or return Confidential Information;
- securely destroy any physical or digital copies;
- certify deletion if reasonably requested.

Exceptions:

- information required by law to be retained;
- backup copies automatically created in systems (deleted on standard cycles);
- data retained for fraud prevention or legal defence (consistent with Section 7).

12.9 Duration of Confidentiality Obligations

Confidentiality obligations:

- begin upon first disclosure;
- continue throughout the term of the Agreement;
- survive termination for **five (5) years**;
- survive indefinitely for trade secrets, source code, algorithms, cryptographic methods and security information.

12.10 Breach of Confidentiality

A breach of confidentiality by either party:

- may cause irreparable harm;
- may entitle the Disclosing Party to seek injunctive relief;
- may entitle the Disclosing Party to damages;
- constitutes a **material breach** of the Agreement;
- may justify suspension or termination under Section 17.

12.11 No Publicity Without Consent

Neither party may:

- publicly announce the existence of the Agreement;
- issue press releases;
- use the other party's name, logo or branding;
- state or imply endorsement;

without prior **written consent**, except where required by law.

SECTION 13 — WARRANTIES

13.1 Mutual Warranties

Each party warrants that:

1. **It has authority to enter into this Agreement.**
   It has full power and legal capacity to enter into, and perform its obligations under, these Terms.
2. **It will comply with applicable laws.**
   Each party will comply with laws and regulations that apply to its performance under this Agreement.
3. **Its personnel are qualified.**
   Individuals acting on behalf of either party are suitably skilled and authorised to perform their responsibilities.

13.2 Veyco's Warranties

Veyco warrants that:

1. **The Services will be provided with reasonable care and skill.**
   Veyco will provide the Services using personnel with appropriate skill and experience, consistent with good industry practice for identity, referencing and e-signature services.
2. **The Platform will function materially in accordance with its documentation.**
   While not guaranteeing uninterrupted availability, Veyco will act reasonably to maintain operational performance.
3. **It will implement appropriate security measures.**
   Veyco will maintain appropriate technical and organisational measures consistent with Section 7 (Data Protection & Privacy).
4. **It will process Personal Data lawfully when acting as a Processor.**
   Veyco will follow the Partner's documented instructions except where otherwise permitted by law or the Agreement.
5. **It will not materially degrade core functionality.**
   Veyco will not intentionally reduce the core identity, referencing or signing capabilities of the Platform without good operational, security or legal reason.

13.3 Partner Warranties

The Partner warrants that:

1. **It has lawful basis for all data it submits.**
   The Partner has obtained all consents, notices, permissions and lawful bases required to instruct Veyco to process User Personal Data.

2. **All information provided to Veyco is accurate.**
   This includes:
   - User contact details
   - tenancy details
   - documents or forms the Partner uploads
   - referencing information requested by the Partner
3. **It will comply with all laws applicable to tenancy decisions.**
   Including:
   - Right to Rent obligations
   - consumer protection laws
   - anti-discrimination laws
   - housing and landlord obligations
   - immigration law
   - data protection law
4. **It will not misuse the Services.**
   Including by:
   - using Reports for unrelated purposes
   - extracting or reselling Veyco data
   - using Veyco data for AI training
   - reverse engineering
   - creating derivative works of the platform
   - benchmarking or competitive analysis
5. **It will maintain secure access controls.**
   Including:
   - protecting API keys
   - managing authorised users
   - promptly revoking access for former staff
6. **It will not upload harmful content.**
   The Partner will not upload documents containing malware, corrupted files or harmful materials.

13.4 User Warranties (Passed Through Partner)

The Partner warrants that it will ensure Users agree that:

1. **All information submitted is truthful and accurate.**
2. **Documents submitted belong to them or they are authorised to use them.**
3. **They will not attempt to bypass verification steps.**
4. **They will not commit fraud or impersonation.**
5. **They will comply with identity verification and signing procedures.**

The Partner shall indemnify Veyco for losses arising from User misrepresentation (in accordance with Section 16).

13.5 No Warranties for Accuracy of Reports

The Partner acknowledges that:

- Veyco does **not** warrant the accuracy, completeness or correctness of Reports;
- Veyco does **not** guarantee detection of all fraudulent documents;
- Veyco does **not** guarantee that identity or biometric verification will always succeed;
- referencing and affordability outputs are **informational only**;
- all decision-making responsibility remains with the Partner.

Reports are not legal, financial, tenancy, immigration or compliance advice.

13.6 No Warranty for Third-Party Providers

Veyco may use third-party services for:

- document analysis
- biometric matching
- identity checks
- email/SMS delivery
- hosting
- certificate authorities
- fraud-prevention tools

Veyco does **not** warrant:

- third-party accuracy, uptime or performance;
- continued availability of any specific provider;
- correctness of third-party database data.

Veyco will use reasonable efforts to select reputable providers and maintain continuity.

13.7 Exclusion of Implied Terms

To the maximum extent permitted by law, Veyco excludes all implied warranties, including:

- merchantability
- fitness for a particular purpose
- non-infringement
- quiet enjoyment
- accuracy of information
- quality or completeness of outputs
- suitability for legal or compliance obligations

Veyco provides the Services **"as is"** except as expressly warranted.

13.8 No Guarantee of Identity, Suitability or Outcomes

The Partner acknowledges that Veyco does not warrant or guarantee:

- the identity of a User;
- that a User is suitable for a tenancy;
- that a User has the legal right to rent or sign a tenancy;
- that a User will comply with any contract;
- that a signed document is enforceable in all circumstances;
- that referencing data is accurate;
- that income documents or supporting materials are genuine;
- that no fraud will occur.

These matters remain the sole responsibility of the Partner.

13.9 Limitation of Warranties

The warranties in this Section:

- are the **only warranties** provided by Veyco;
- replace all other warranties (express or implied);
- operate subject to Section 15 (Liability & Liability Cap).

SECTION 14 — LIABILITY & LIMITATION OF LIABILITY

14.1 General Liability Principles

Each party is responsible for:

- its own acts and omissions;
- the acts and omissions of its employees and contractors;
- complying with applicable laws; and
- ensuring its use of the Services is lawful and appropriate.

Nothing in these Terms excludes or limits liability where doing so would be unlawful.

14.2 Liability That Cannot Be Excluded

Nothing in these Terms limits or excludes either party's liability for:

1. **death or personal injury caused by negligence**;
2. **fraud or fraudulent misrepresentation**;
3. **any liability which cannot legally be excluded under applicable law**;
4. **wilful misconduct**.

These remain fully uncapped.

14.3 Veyco Is Not Liable For Certain Categories of Loss

To the fullest extent permitted by law, Veyco shall **not** be liable for:

14.3.1 Business Consequential Losses

- loss of profits;
- loss of revenue;
- loss of business or business opportunities;
- loss of anticipated savings;
- loss of goodwill;
- loss of reputation;
- business interruption.

14.3.2 Data or Output-Related Losses

- loss, corruption or inaccuracy of Reports or data (except where caused by Veyco's breach of Data Protection Laws);
- decisions made or actions taken based on Reports, referencing outputs or verification results;
- any inferences drawn by the Partner from Veyco's tools.

14.3.3 Identity, Referencing or Verification-Related Losses

Veyco is not liable for:

- identity fraud successfully carried out by a User;
- forged or altered documents the system does not detect;
- errors, omissions or misrepresentations by Users;
- employment or landlord references that are false or incomplete;
- incorrect affordability information submitted by Users;
- Right to Rent non-compliance resulting from Partner action or inaction;
- tenancy decisions or financial losses arising from Partner reliance on a Report.

14.3.4 Third-Party Failures

Veyco is not liable for failures of:

- biometric engines;
- document verification providers;
- certificate authorities;
- Share Code services or Home Office systems;
- email/SMS delivery systems;
- cloud hosting services;
- telecoms or internet access.

14.3.5 Indirect or Special Damages

Veyco is not liable for any special, exemplary, indirect or consequential damages.

14.4 Partner Responsibility for Decisions

The Partner is solely responsible for:

- tenancy decisions;
- assessing affordability;
- verifying employment history;
- evaluating guarantor suitability;
- interpreting Reports;
- reviewing documents;
- complying with Right to Rent, consumer protection and discrimination laws;
- legal compliance and professional advice.

Veyco is **not** responsible for the Partner's:

- tenancy outcomes,
- legal compliance, or
- use of Reports for decision-making.

14.5 Liability Cap

Subject to Sections 15.1 and 15.2:

Veyco's total aggregate liability arising out of or in connection with the Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, shall not exceed:

the total Fees paid or payable by the Partner to Veyco in the six (6) months immediately preceding the date on which the claim arose.

If the Agreement has been in force for less than six months, the cap is:

the total Fees paid or payable up to the date of the claim.

This is the **maximum** liability for **all** claims combined.

14.6 Liability for Data Protection Breaches

For clarity:

- Veyco remains liable for **its own breach** of Data Protection Laws where acting as a Controller;
- where acting as a Processor, Veyco is liable only to the extent required by UK GDPR;
- Partner remains liable for ensuring lawful basis and correctness of instructions;
- Veyco is not liable for any unlawful or incorrect instructions given by the Partner.

Data Protection liability remains subject to the **6-month liability cap** unless excluded under Section 15.2.

14.7 Increased Risk Areas (Not Covered by Veyco Liability)

Veyco is not responsible for losses arising from:

- Partner misuse of API keys;
- insecure Partner IT infrastructure;
- Partner's failure to secure access credentials;
- failure to follow instructions or guidance;
- use of the Services for unsupported or unlawful purposes;
- modifications, integrations or third-party systems connected by the Partner.

14.8 Liability for User Fraud

Veyco is not liable for:

- identity fraud,
- impersonation,
- presentation attacks,
- forged documents,
- falsified employment references,
- altered bank statements,
- or any deception carried out by Users.

Identity and referencing checks reduce risk but **do not eliminate it**.

14.9 Time Limit for Bringing Claims

Any claim by either party must be brought within:

12 months of the date on which the claiming party first became aware of the issue,

after which the claim is permanently barred.

14.10 Apportionment of Risk

Both parties acknowledge that:

- the Fees reflect the allocation of risk in these Terms;
- without the limitations in this Section, the Services could not be offered at the agreed pricing;
- the Partner is responsible for verifying critical information independently;
- identity, referencing and signing outcomes inherently involve operational uncertainty.

14.11 Multiple Claims

Multiple claims arising from:

- the same issue,
- the same series of events, or
- a continuous problem

will count as **one claim** for the purposes of applying the liability cap.

SECTION 15 — INDEMNITIES

15.1 Partner Indemnities (Primary Indemnity Obligations)

The Partner shall indemnify, defend and hold harmless Veyco, its officers, directors, employees, agents and subcontractors ("**Veyco Indemnified Parties**") from and against any and all losses, damages, liabilities, penalties, fines, costs and expenses (including reasonable legal fees) arising out of or relating to:

15.1.1 Misuse of the Services

Any misuse, improper use, or unauthorised use of:

- identity verification workflows,
- referencing tools,
- QES signing flows,
- the Platform,
- the API,
- Reports,
- audit trails, or
- Veyco data.

15.1.2 Unlawful or Incorrect Instructions

Any processing carried out by Veyco **on the Partner's instructions** where:

- the instructions are unlawful;
- the Partner failed to have a lawful basis;
- the Partner failed to obtain necessary notices or consents;
- the instructions violate Data Protection Laws;
- the Partner instructed processing of a User who did not give required consent (e.g., biometrics).

15.1.3 User Misrepresentation, Fraud or Misconduct

Any losses arising from:

- fraudulent or falsified documents submitted by Users;
- identity fraud or impersonation;
- inaccurate, misleading or untrue User information;
- forged signatures or false declarations;
- manipulation of documents, images or video captures.

Veyco is not responsible for User actions. The Partner indemnifies Veyco for all resulting

losses.

15.1.4 Partner's Breach of Law

Any Partner breach of:

- Right to Rent requirements;
- consumer protection laws;
- discrimination laws;
- data protection laws;
- housing or tenancy laws;
- financial crime or fraud-prevention legislation.

15.1.5 Uploaded Content

Any claim relating to Partner Content:

- infringing third-party rights;
- being inaccurate, unlawful or defamatory;
- violating copyright, contract or privacy laws;
- introducing viruses or malicious code.

15.1.6 Partner's Integration, Infrastructure or Security Failures

Any claim arising from:

- insecure API key management;
- improper configuration of Partner systems;
- third-party vendors engaged by the Partner;
- breach of the Partner's systems or environment;
- failure to implement adequate technical or organisational measures.

15.1.7 Authorised Users and Contractors

Any act or omission of:

- Partner employees,
- contractors,
- agents,
- system integrators, or
- its own Users,

using or accessing the Services via the Partner's account or API credentials.

15.2 Veyco Indemnities (Controlled Narrow Scope)

Veyco shall indemnify, defend and hold harmless the Partner against losses, damages and reasonable legal fees **solely** to the extent arising from:

15.2.1 IP Infringement by the Platform

A third-party claim that the Platform (excluding any Partner Content, User Content or third-party components) infringes a valid:

- patent,
- copyright,
- trademark, or
- other Intellectual Property Right.

15.2.2 Conditions of the IP Indemnity

The indemnity in 16.2.1 applies only if:

- the Partner promptly notifies Veyco in writing of the claim;
- Veyco has sole control over defence and settlement;
- the Partner provides reasonable cooperation and assistance;
- the Partner does not prejudice the defence (e.g., by making admissions).

Veyco may, at its discretion:

- obtain the right for the Partner to continue using the Services;
- replace or modify the Services to avoid infringement;
- terminate the affected portion of the Services and refund pre-paid Fees for the unused period.

15.3 Exclusions to Veyco's IP Indemnity

Veyco's indemnity **does not** apply to claims arising from:

- Partner Content or User Content;
- Partner modifications;
- third-party systems integrated by the Partner;
- use of the Services outside the permitted scope;
- breach of these Terms by the Partner;
- use of old or outdated versions of the API or Platform;
- compliance with the Partner's instructions or branding.

15.4 Indemnities for Data Protection Issues

15.4.1 Partner Indemnity (Data Protection)

The Partner shall indemnify Veyco for:

- unlawful or incorrect processing instructions;
- failure to meet transparency obligations;
- lack of lawful basis;
- misrepresentation of purposes to Users;
- mishandling User rights requests;
- security breaches in the Partner's systems;
- failure to comply with Right to Rent or immigration requirements.

15.4.2 Veyco Indemnity (Data Protection)

Veyco shall indemnify the Partner **only** to the extent that:

- Veyco, acting as Controller,
- commits a proven breach of Data Protection Laws,
- which directly causes loss to the Partner.

This indemnity remains subject to the liability cap in **Section 15**.

15.5 Indemnity for Third-Party Claims

The Partner indemnifies Veyco for third-party claims arising out of:

- tenancy decisions;
- referencing outcomes;
- signature validity disputes between the Partner and Users;
- employment or landlord reference disputes;
- User complaints relating to the Partner's decisions;
- failure by the Partner to comply with legal or professional duties.

Veyco is not responsible for tenancy suitability judgments or legal compliance.

15.6 Indemnity Procedures

The following apply to all indemnities:

1. **Prompt Notification**
   The indemnified party must notify the indemnifying party as soon as reasonably possible after becoming aware of a claim.

2. **Control of Proceedings**
   The indemnifying party has sole control over the defence and settlement of the claim.
3. **Cooperation**
   The indemnified party must provide reasonable cooperation and information.
4. **Mitigation**
   Both parties must take reasonable steps to mitigate losses.
5. **No Admissions**
   The indemnified party must not admit liability or settle without written consent.

15.7 Relationship to Liability Cap

Except for indemnities that cannot legally be capped (e.g., fraud), all indemnities given by either party are:

- subject to the liability limitations in **Section 15**, including
- the **6-month total Fees paid** liability cap.

SECTION 16 — SUSPENSION & TERMINATION

16.1 Suspension of the Services

Veyco may temporarily suspend or restrict access to the Services (including API access) immediately and without liability if:

16.1.1 Security or Fraud Risk

Veyco reasonably believes that:

- the Partner's account has been compromised;
- API keys have been exposed;
- suspicious or fraudulent activity is occurring;
- Users are attempting to bypass verification;
- documents have been manipulated;
- misuse of the Services is taking place.

16.1.2 Legal or Regulatory Requirement

Suspension is required to:

- comply with law,
- comply with a regulator or government request,
- prevent unlawful activity, or
- enforce immigration or fraud-prevention obligations.

16.1.3 Non-Payment

The Partner fails to pay undisputed Fees when due.

16.1.4 Technical Issues

Suspension is necessary to:

- protect platform integrity,
- prevent data loss,
- address critical vulnerabilities, or
- maintain system stability.

16.1.5 Breach of the Agreement

The Partner:

- breaches these Terms,
- misuses the Services,
- breaches Data Protection Laws,
- fails to comply with access restrictions.

Suspension will be for the minimum period required to resolve the issue.

16.2 Effects of Suspension

During suspension:

- Veyco may restrict Dashboard access;
- Veyco may block API calls;
- identity checks and referencing may be prevented;
- signing workflows may not be initiated;
- access to Reports may be restricted.

Suspension does **not**:

- waive or reduce Fees owed;
- terminate the Agreement;
- entitle the Partner to compensation.

Veyco will reinstate access once the cause of suspension is resolved.

16.3 Termination by the Partner

The Partner may terminate the Agreement:

1. **for convenience**, by providing 30 days' written notice;
2. **for material breach** by Veyco that is not remedied within 30 days of written notice;
3. **if Veyco becomes insolvent** or ceases trading.

Termination for convenience does not entitle the Partner to a refund of Fees already paid.

16.4 Termination by Veyco

Veyco may terminate the Agreement immediately upon written notice if:

1. **the Partner fails to pay undisputed Fees** within 30 days of the due date;
2. **the Partner misuses the Services**, including identity, referencing, signing or API tools;
3. **the Partner materially breaches** these Terms and fails to remedy the breach within 30 days;
4. **continuing the Agreement would violate law**, regulatory obligations or fraud-prevention duties;
5. **the Partner becomes insolvent**, enters administration, or ceases trading;
6. **Veyco reasonably determines** that providing the Services to the Partner creates:
    - unacceptable fraud risk,
    - legal risk, or
    - reputational risk.

16.5 Automatic Termination

The Agreement automatically terminates if:

- the Partner's account is inactive for more than 12 months;
- the Partner cancels their subscription or plan;
- the Partner's access is revoked due to non-payment and not reinstated within 60 days.

Veyco may, at its discretion, notify the Partner prior to automatic termination.

16.6 Consequences of Termination

Upon termination:

16.6.1 Access Ceases

The Partner must immediately cease all:

- use of the Platform;
- use of the API;
- initiation of identity checks;
- initiation of referencing workflows;
- initiation of signing workflows.

16.6.2 Deletion of Access Credentials

Veyco will deactivate:

- Partner Dashboard access,
- administrative accounts,
- API keys.

16.6.3 Fees Remain Payable

The Partner must pay:

- all outstanding invoices;
- all Fees for checks performed prior to termination;
- any late payment charges accrued.

Termination does not reduce or waive fees owed.

16.6.4 Data Retention and Deletion

Veyco will:

- retain or delete Personal Data in accordance with Section 7;
- delete Partner-specific configuration or integration settings;
- retain audit logs, evidence files and Right to Rent records where legally required.

16.6.5 Retrieval of Documents

If requested within 30 days of termination:

- Veyco will provide reasonable access to download Reports, signed documents and certificates;
- Veyco may charge an administrative fee for bulk export.

After this period, Veyco has no obligation to retain or provide access.

16.7 Survival of Obligations

The following sections survive termination:

- Section 7 (Data Protection & Privacy)
- Section 10 (Reports & Reliance)
- Section 11 (Audit Trails)
- Section 12 (Intellectual Property)
- Section 13 (Confidentiality)
- Section 14 (Warranties)

- Section 15 (Liability)
- Section 16 (Indemnities)
- Section 17 (Termination Consequences)
- Section 18 (Governing Law)
- Section 19–21 (General Provisions)

16.8 No Liability for Termination

Neither party shall be liable for damages resulting solely from:

- lawful termination under this Section;
- suspension made in accordance with these Terms.

However, the Partner remains liable for:

- all Fees incurred;
- indemnity obligations;
- breaches occurring prior to termination.

SECTION 17 — GOVERNING LAW & JURISDICTION

17.1 Governing Law

These Terms, and any non-contractual obligations arising out of or in connection with them, shall be governed by and construed in accordance with the laws of:

England and Wales.

17.2 Jurisdiction

Each party irrevocably agrees that the courts of:

England and Wales

shall have **exclusive jurisdiction** to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with:

- these Terms,
- the Services,
- any verification or referencing activities,
- electronic signature workflows,
- Reports or outputs,
- or the use of the Platform.

17.3 Exception for Injunctive Relief

Nothing in this Section prevents either party from seeking:

- urgent interim relief,
- injunctive relief, or
- equitable remedies

in any jurisdiction where the other party has assets or where relief is required to prevent immediate harm.

17.4 Consumer Rights (If Applicable)

Where the Partner uses the Services for business purposes, consumer laws do **not** apply.

If the Partner allows or facilitates consumer Users to access the Platform, this does not change the governing law or jurisdiction between Veyco and the Partner.

SECTION 18 — NOTICES

18.1 How Notices Must Be Given

Any notice or other communication given under or in connection with these Terms must be:

- **in writing**, and
- delivered by one of the following permitted methods:
    1. **email**,
    2. **hand-delivery**, or
    3. **registered or tracked post**.

Notices given by instant messaging platforms (e.g., WhatsApp, SMS, Slack) are **not valid** unless explicitly agreed in writing by both parties.

18.2 Notices to Veyco

Notices to Veyco must be sent to:

Legal Notices Email:
compliance@veyco.com

Registered Address:
Veyco Ltd
Department Campfield
Lower Byrom Street
Manchester M3 4FP

Notices sent to outdated or incorrect addresses are not considered delivered unless Veyco confirms receipt.

18.3 Notices to the Partner

Notices to the Partner will be sent to:

- the email address associated with the Partner's account;
- or any email address designated in writing by the Partner;
- or, if required, to the Partner's registered or trading address.

The Partner is responsible for ensuring that:

- their email address is valid,
- mailboxes accept Veyco emails,
- notice recipients monitor their inbox,
- changes of address are communicated promptly.

18.4 When Notices Are Deemed Delivered

Notices are deemed delivered as follows:

18.4.1 Email

- **When sent**, provided no bounce-back or failure message is received;
- or **at 9:00am** (UK time) on the next Business Day if sent outside business hours.

18.4.2 Hand Delivery

- At the time of delivery, as evidenced by signature or timestamp.

18.4.3 Registered/Tracked Post

- At **9:00am** on the **second Business Day** after posting, or
- when delivery is confirmed by tracking (whichever is earlier).

18.5 Notices Relating to Suspension or Termination

Notices relating to:

- material breach,
- suspension under Section 17,
- termination of the Agreement,

may be issued by email only (no requirement for postal notice unless legally required).

Email is fully valid for enforcement notices.

18.6 Changes to Contact Details

Either party may update its notice details by giving written notice to the other party.

Changes take effect:

- immediately upon receipt (for email), or
- on deemed delivery (for post).

Until then, notices sent to existing details remain valid.

18.7 Service of Legal Proceedings

Service of proceedings may only be made:

- by tracked post,
- by courier requiring signature, or
- by email (if expressly agreed and acknowledged).

Nothing prevents a party from serving proceedings via any method permitted under the Civil Procedure Rules.

SECTION 19 — CHANGES TO THESE TERMS

19.1 Right to Update or Amend

Veyco may update or amend these Terms from time to time to reflect:

- changes to the Services;
- updates to identity, referencing, biometric or QES workflows;
- improvement of security or fraud-prevention methods;
- changes to third-party verification providers;
- new features or functionality;
- changes in applicable laws or regulations;
- operational or technical requirements;
- corrections, clarifications or improvements to wording.

Changes may be made **at Veyco's discretion**, but always in compliance with law.

19.2 Notice of Material Changes

Where changes are **material** (e.g., affecting rights, responsibilities or pricing), Veyco will:

- notify the Partner by email,
- or notify via an in-platform message,
- or notify through a prominent notice on the Dashboard.

Material changes will take effect:

- **30 days after** the date of notification, unless a shorter period is required by law or security concerns.

19.3 Non-Material or Operational Changes

Changes that:

- improve security,
- fix errors,
- update sub-processors (within allowed scope),
- modify workflows without reducing functionality,
- reflect infrastructure updates, or
- add optional features,

may be made without notice.

These changes do not materially affect the Partner's rights or obligations.

19.4 Partner's Right to Object

If the Partner reasonably believes a material change adversely affects them, they may:

- contact Veyco to discuss the change;
- request clarification;
- or terminate the Agreement by giving written notice before the change takes effect.

Termination does not entitle the Partner to a refund of Fees already paid unless required by law.

19.5 Continued Use Constitutes Acceptance

Continued use of the Platform or Services **after the effective date** of any updated Terms constitutes acceptance of the updated Terms.

If the Partner does not agree to the updated Terms, they must stop using the Services before the effective date.

19.6 Changes Required by Law

If laws, regulations or regulatory guidance require immediate changes:

- the updated Terms may take effect **immediately**;
- Veyco will notify the Partner as soon as reasonably practicable;
- such changes do not constitute a breach of the Agreement.

19.7 Updates to Policies and Documentation

Veyco may update:

- the Privacy Policy;
- API documentation;
- acceptable use rules;
- technical specifications;
- onboarding instructions;

without prior notice, provided changes:

- do not materially diminish the Services, and
- remain consistent with these Terms.

19.8 Record of Changes

Veyco may maintain a version history of Terms and policies, which may include:

- effective dates;
- summaries of major changes;
- archived versions.

This may be published on the Veyco website or supplied upon request.

SECTION 20 — GENERAL PROVISIONS

20.1 Entire Agreement

These Terms, together with any documents expressly incorporated by reference (including the Privacy Policy, Data Processing Agreement, and any written commercial agreement) constitute the **entire agreement** between the parties and:

- supersede all prior proposals, negotiations, understandings or representations (whether written or oral);
- prevail over any terms or purchase orders submitted by the Partner unless expressly agreed in writing.

No other terms apply unless Veyco expressly agrees in writing.

20.2 Assignment

20.2.1 By the Partner

The Partner may not:

- assign,
- transfer,
- subcontract,
- delegate, or
- novate

any of its rights or obligations under these Terms **without Veyco's prior written consent** (not to be unreasonably withheld).

20.2.2 By Veyco

Veyco may assign or transfer its rights or obligations:

- to an affiliate,
- to a purchaser of its business,
- to a corporate successor, or
- to a service provider involved in delivering the Services,

provided such entity agrees to honour the Terms.

20.3 Subcontracting

Veyco may subcontract any part of the Services, including:

- hosting providers,
- identity verification engines,
- biometric or document analysis tools,

- certificate authorities,
- fraud-prevention providers,
- customer support partners.

Veyco remains responsible for subcontractors' performance as if it had performed the services itself.

20.4 Force Majeure

Neither party is liable for delay or failure to perform obligations (other than payment obligations) caused by events outside its reasonable control, including:

- natural disasters;
- power failures;
- civil unrest;
- pandemics;
- telecommunications outages;
- government actions;
- industrial action;
- failures of third-party infrastructure.

During a Force Majeure event:

- obligations are suspended;
- parties will work to minimise disruption;
- if the event continues for more than 60 days, either party may terminate on written notice.

20.5 No Partnership or Agency

Nothing in these Terms shall:

- create a partnership,
- joint venture,
- employment relationship, or
- agency relationship.

Neither party has authority to bind the other except as expressly permitted in these Terms.

20.6 No Third-Party Rights

Except for persons indemnified under Section 16, these Terms do **not** give rise to any rights for any third party under the Contracts (Rights of Third Parties) Act 1999.

A third party cannot enforce or rely on any term of this Agreement.

20.7 Severability

If any provision of these Terms is found by a court of competent jurisdiction to be:

- invalid,
- unlawful, or
- unenforceable,

the remaining provisions shall remain in full force and effect.

The invalid provision will be replaced by a lawful and enforceable provision that most closely matches the intent of the original.

20.8 Waiver

Failure by either party to:

- enforce any provision,
- exercise any right, or
- insist on performance of obligations,

does **not** constitute a waiver of those rights.

A waiver is only valid if given explicitly in writing.

20.9 Amendments

Except as allowed by **Section 20 (Changes to These Terms)**:

- no amendment is effective unless in writing and signed by both parties.

Electronic signatures are valid for amendments.

20.10 Interpretation

In interpreting these Terms:

- "including", "include" and similar expressions are deemed to mean "including without limitation";
- references to statutes include updates or replacements;
- headings are for convenience only and do not affect interpretation;
- references to "writing" include email but not instant messaging;
- references to "person" include corporations and unincorporated bodies.

20.11 Order of Precedence

If there is a conflict between the following, the order of precedence is:

1. Any written commercial agreement or Order Form signed by both parties;
2. These Terms;
3. The Privacy Policy;
4. The Data Processing Agreement;
5. Any API documentation or technical specifications.

20.12 Survival

The following provisions survive termination:

- payment obligations;
- confidentiality;
- data protection;
- intellectual property;
- warranties;
- liability & limitation of liability;
- indemnities;
- audit trails & evidence;
- governing law & jurisdiction;
- general provisions.

20.13 Execution

These Terms may be executed or accepted electronically, including:

- electronic signatures,
- click-wrap acceptance,
- creation of a Partner account, or use of the Services.

Such acceptance has the same legal effect as a handwritten signature.

20.14 Counterparts

If these Terms are signed:

- they may be executed in any number of counterparts;
- each counterpart constitutes an original;
- all counterparts together constitute a single agreement.