# Portal Privacy Notice

**CAB Group – Privacy Notice (Client Onboarding Portal)**

**Effective date:** 1st April 2026

This Privacy Notice explains how CAB Group ("CAB", "we", "us", "our") collects and uses personal data when your organisation uses the CAB's Client Onboarding Portal (the "Portal"). It applies to personal data relating to individuals connected to our corporate clients and prospective clients (for example, directors, shareholders, beneficial owners, authorised signatories and contact persons).

## 1) Who we are and how to contact us

### Who we are

- CAB Group company(ies) identified during onboarding act(s) as independent controller(s) for the processing described in this notice.
- Where CAB performs checks on behalf of a Client as Processor, the Client acts as Controller, and CAB processes personal data strictly in accordance with the Client's instructions and in accordance with the Portal User Terms.

### How to contact us

If you have any questions about this privacy policy or about the use of your personal data or you want to exercise your privacy rights, please contact our DPO in the following ways:

- Email address: dataprotection@crownagentsbank.com
- Postal address: Data Protection Officer, 3 London Bridge St, London SE1 9SG
- Telephone number: +44 (0) 7739 89 9647

**Crown Agents Bank Limited and CAB Payments Holdings plc**

DPO Shabana Uddin

Email: Shabana.Uddin@crownagentsbank.com

**CAB Europe**

Internal Data Protection Officer: Mr. Edwin Weller

E-mail: dataprotection@cabeurope.com

Phone: +31 (0)20 899 6518

Post: Gustav Mahlerplein 2, 1082 MA, Amsterdam, NL.

External data protection authority**:** You may want to submit a tip-off or a complaint to the Autoriteit Persoonsgegevens (AP), the Dutch data protection authority when you have experienced something or that you suspect that a person or an organisation does not comply with the privacy law. Please follow: https://www.autoriteitpersoonsgegevens.nl/en/submitting-a-tip-off-or-a-complaint-to-the-ap

**Crown Agents Global Markets (UAE)**

For the ADGM DPO details, please see below:

Name: Fathima Valiyaveettil Nooh

Email: dataprotection@cabglobalmarkets.com

If you are a data subject of Crown Agents Global Markets (ADGM entity), you have the right to make a complaint to the ADGM Commissioner of Data Protection if we are unable to satisfactorily resolve your complaint.

Telephone : +971 23338888

Address : ADGM Office of Data Protection, ADGM Authorities Building, ADGM Square, Al Maryah Island, PO Box 111999, Abu Dhabi ,UAE

**Complaints**

You have the right to make a complaint to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). However, before doing so please make sure you have first made your complaint to us or asked us for clarification if there is something you do not understand. You can contact us via our contact form on the Crown Agents Bank website.

**2) What data we collect**

We collect and process the following categories of personal data submitted by your organisation or generated through checks:

- Identification & KYC data: full name, date of birth, nationality, country of residence, residential address, contact details, job title/role, relationship to the Client.
- Ownership & governance data: shareholding/beneficial ownership, control and management information, organisational role(s).
- Identity documentation: copies of passports, driving licences, national ID cards, visas/permits, proof of address (e.g., utility bills).
- Compliance screening data: sanctions, politically exposed person (PEP) status, adverse media results, fraud/financial crime indicators.
- Technical & audit data: IP address, device/browser information, login timestamps, activity logs, access records, file metadata.
- Communications: messages, queries, or support tickets relating to the Portal.
- Special category data (only if necessary and lawful): e.g., biometric verification results or liveness checks from identity providers (we do not typically retain biometric templates; see Section 6).

We do not ask for more data than we need. If we ever require additional information, we will explain why.

**3) Sources of data**

- Information you/your organisation provide directly via the Portal or during onboarding.
- Public sources (e.g., corporate registries, gazettes, sanctions lists, reliable databases).

- Trusted third-party providers for identity verification, sanctions/PEP/adverse media screening, and document authentication.
- Other CAB Group companies where needed for onboarding, risk management, or service delivery.

**4) Purposes and lawful bases**

We process personal data for the following purposes and under these lawful bases under the UK GDPR:

| Purpose | Lawful basis |
|---|---|
| Onboarding and KYC/AML/CTF due diligence, risk assessment, sanctions/PEP screening, fraud prevention | Legal obligation (e.g., Money Laundering Regulations), Public interest in preventing financial crime (where applicable), and Legitimate interests in ensuring the integrity of our counterparties |
| Contract setup and management, authorising signatories, ongoing relationship management | Contract (to take steps at your request or perform a contract), Legitimate interests (efficient service provision) |
| Ongoing monitoring and periodic refresh of due diligence | Legal obligation, Legitimate interests (risk management and compliance) |
| Security, audit trails, incident detection and prevention | Legitimate interests (platform and data security), Legal obligation (where applicable) |
| Regulatory and law enforcement requests, recordkeeping | Legal obligation |
| Service improvement, troubleshooting, analytics (aggregate/de-identified where possible) | Legitimate interests (improving services and Portal performance) |

Special category data (if any): Only processed where necessary and based on a valid condition (e.g., substantial public interest for preventing or detecting unlawful acts; or explicit consent where we rely on biometrics via a third-party IDV provider). We will clearly indicate where such processing applies.

**5) Sharing your data**

We may share personal data with:

- CAB Group companies for onboarding, risk management, compliance and service delivery on a “need-to-know” basis.
- Trusted service providers acting under contract (e.g., hosting, cloud storage, KYC/ID verification, sanctions/PEP/adverse media screening, email/security operations, support).
- Professional advisers (lawyers, auditors, insurers) under confidentiality obligations.
- Regulators, law enforcement, and courts where required by law or to protect rights, security and integrity.
- Transaction counterparties (e.g., where required during mergers, acquisitions or corporate restructuring) under appropriate safeguards.

We do not sell personal data.

**6) International transfers**

Your data may be processed in the UK, the EEA, and (if required) in countries outside the UK/EEA. Where we transfer data internationally, we implement appropriate safeguards, such as:

- UK IDTA or UK Addendum to EU Standard Contractual Clauses;

- Adequacy regulations/decisions for destination countries;
- Additional technical and organisational measures (e.g., encryption in transit and at rest, access controls).

**7) Third-party providers used for KYC/hosting**

- Hosting & infrastructure: Microsoft D365 and Azure
- ID verification & document authentication: Microsoft D365 and Azure
- Sanctions/PEP/adverse media screening: Eastnets platform, powered by Dow Jones
- Security monitoring & logging: Microsoft D365 and Azure

We maintain contracts imposing confidentiality, security and data protection obligations on these providers.

**8) Retention**

We retain personal data for as long as necessary for the purposes set out in this notice, including to satisfy legal/regulatory retention obligations (e.g., AML recordkeeping) and to establish or defend legal claims. Typical retention periods:

- KYC/AML records: generally, 6 years after the end of the relationship or the date of the last transaction, unless law requires longer/shorter.

- Portal access logs and security records: Sign in logs are getting stored for 1 month on Azure Entra Portal. This is max duration.

- Contract/relationship records: for the applicable statutory limitation periods.

We will securely delete or anonymise data once retention ends.

**9) Security**

We apply appropriate technical and organisational measures to protect personal data, including:

- Encryption in transit and at rest (where applicable);
- Role-based access controls and least-privilege access;
- Multi-factor authentication for administrative access;
- Network segregation, vulnerability management and monitoring;
- Audit logging and incident response procedures;
- Supplier due diligence and contractual security obligations.

No system can be guaranteed 100% secure; we maintain layered controls and continuously improve our security.

**10) Your rights**

Depending on the circumstances and legal basis, individuals have rights under the UK GDPR, including:

- Access to their personal data and information about how it is used;
- Rectification of inaccurate or incomplete data;
- Erasure (right to be forgotten) in certain situations;
- Restriction of processing in certain situations;
- Objection to processing based on legitimate interests or public interest;
- Portability (receive data in a structured, commonly used format) where processing is by automated means and based on consent or contract;

- Withdraw consent (where consent is relied upon) at any time;
- Not be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects, unless lawful safeguards apply.

To exercise rights, contact us using the details in Section 1. We may need to verify identity and scope.

**11) Automated decision-making and profiling**

- Screening and risk scoring: We may use automated tools for sanctions/PEP/adverse media screening and risk scoring to support compliance assessments.
- Human oversight: Any decision with legal or similarly significant effects is subject to human review; we do not make such decisions solely by automated means.

**12) Cookies and similar technologies**

The Portal may use necessary cookies (for authentication, security, and session integrity) and, if you choose to allow them, analytics cookies to improve performance.

- See our Cookie Notice for details of cookie names, purposes and durations.
- You can manage preferences through the Portal's cookie controls and your browser settings.

**13) Your responsibilities (corporate clients)**

In accordance with the Portal User terms, your organisation is responsible for:

- Ensuring the individuals whose data is submitted are informed about this processing (including by providing them with this Privacy Notice);
- Providing accurate and up-to-date information;
- Only submitting data that is necessary and lawfully obtained;
- Managing authorised user access and credentials for the Portal.

**14) Changes to this notice**

We may update this Privacy Notice from time to time. Material changes will be notified via the Portal or by email. Please review this page periodically.