Privacy Notice - Vendors

ABOUT THIS NOTICE

You are receiving this notice because Crown Agents Bank Limited (“we”, “our”, “us”) or a member of the CAB Group (collectively referred to as “CAB”), procures certain services ("Services") from you (the "Supplier", "you" or "your"), and you provide those Services as an CAB Approved Vendor. As part of our Supplier onboarding due diligence process, we collect and process certain personal information about key individuals associated with our Suppliers – specifically ultimate beneficial owners (UBOs) and company directors.

CAB Group (Group) is made up of different legal entities, details of which can be found on the Crown Agents Bank website.

All personal data is handled in accordance with the UK Data Protection Act 2018, EU General Data Protection Regulation (collectively, "GDPR") and The Privacy and Electronic Communications Regulations (PECR).

The purpose of this privacy notice is to inform you as to how we look after your personal data when you provide information to CAB in accordance with CAB’s onboarding process which is completed either via email, website, or designated vendor portal.

This notice sets out your privacy rights and how the law protects you. It is important that you read this privacy notice so that you are fully aware of how and why we are using your data. When Crown Agents Bank Limited processes your data for these purposes, it is a "data controller" as defined within GDPR. This means that we are responsible for how we use the personal data we hold about you.

If you have any questions about this privacy notice or wish to exercise your privacy rights as set out in this notice, please contact our Data Protection Officer using the contact details as set out below.

This notice also applies to authorised signatories, finance contacts, employees of our Suppliers and other personnel of your organisation involved in the supply relationship.

OUR COLLECTION AND USE OF YOUR PERSONAL INFORMATION

We collect and process certain personal information about key individuals associated with our Suppliers – specifically ultimate beneficial owners (UBOs) and company director details. This data is supplied by you through completion of our Vendor Registration Form. We do this to satisfy our legal and regulatory due diligence obligations (for example, anti-money laundering, financial crime and know-your-supplier requirements). This ensures we comply with applicable laws and engage only with legitimate, compliant business partners.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- Identity data, which includes full name, date of birth, nationality, domicility and information on shareholding or directorship roles.
- Contact data, which includes your email address, phone number or other contact information provided by you.

We process data where necessary for our legal obligations under anti-money laundering and sanctions laws (Article 9(2)(g) GDPR and Article 10 of the UK Data Protection Act 2018) and in accordance with our Group Data and Management Policy, with safeguards including access restrictions, minimisation and limited retention.

We may also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. If we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this notice.

HOW WE USE YOUR PERSONAL DATA

We typically collect and use your personal data for the following purposes:

- To perform all requisite due diligence as a regulated firm ahead of procuring goods or services from Suppliers.
- To provide on-going assurance that entities are fit and proper partners within our supply chain.
- To identify any malfeasance or breach of sanctions and locally applicable legislation.

We rely on specific legal bases tailored to each processing activity: contractual necessity for onboarding; legitimate interests for ongoing Supplier relationship management; legal obligations to perform mandatory anti-money laundering, sanctions and fraud screening; and consent for optional sustainability and marketing communications subject to your separate opt-in in accordance with PECR.

Over and above the Legitimate Interest 'Lawful Basis' for collection of data to satisfy our regulatory obligations, Crown Agents Bank – as a B Corp Certified company committed to high standards of social and environmental impact – proactively engages with its supplier base to both nurture and encourage responsible supply-chains and sustainable procurement.

In furtherance of these efforts, we would like to periodically contact you in order to offer updates on the steps we are taking and invitations on how you can help us meet these goals, including opportunities to undertake CAB-Funded United Nations Global Compact (UNGC) Sustainability Training.

Whilst encouraged, your participation in these initiatives is not mandatory, nor will participation or lack thereof influence or prejudice your firm's selection, or continued use, by Crown Agents Bank (or its subsidiaries and representative offices).

Should you not wish to participate in any such activity please ensure that this is indicated on the Vendor Registration Form. If you subsequently wish to start or cease participation, please contact our Data Protection Officer as indicated below.

CHANGE OF PURPOSE

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

PROVIDING INFORMATION TO THIRD PARTIES

We will not share your personal data with any third parties outside our organisation unless it is required by law or strictly necessary for us to fulfil our compliance obligations. This means we do not sell, trade, or casually disclose your information to external entities for their own purposes. However, in some cases we may need to provide certain details to outside parties for compliance reasons – for example, we might disclose information if required to do so by a government regulator or law enforcement, or to a specialised screening service that helps us perform mandatory legal checks. In all such cases, we ensure any transfer of data is lawful, minimal, and only done for the specific purpose of meeting our

legal requirements. Aside from these exceptions, your personal information remains within our organisation.

TRANSFER OF YOUR PERSONAL DATA OUT OF THE EEA

We do not typically need to transfer any of your personal data to which this notice applies outside the UK and/or the EEA, but this may happen in connection with some Services. If we transfer personal data covered by this notice to external third parties based who are not in the UK and are outside the EEA, we will ensure that adequate safeguards are in place, as required under GDPR. For example, we rely on EU Standard Contractual Clauses, the UK International Data Transfer Agreement and adequacy decisions for transfers to third countries.

DATA RETENTION

We retain onboarding and identity data for the duration of our business relationship plus seven years to satisfy audit obligations; we retain criminal conviction, sanctions and PEP screening results for five years; and we retain other personal information for seven years after our relationship ends, or as required by law. The periods are determined based on the amount, nature and sensitivity of the data, risk of harm from unauthorised use, and applicable legal requirements.

DATA SECURITY

We have put in place security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

We implement technical and organisational measures such as encryption at rest and in transit, strict access controls, regular penetration testing, disaster recovery procedures and comprehensive staff training to safeguard your personal data.

PROCESSING IN LINE WITH YOUR RIGHTS UNDER THE GDPR

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below);
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground;

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- Request the transfer of your personal information to another party.
- Withdraw consent in the circumstances where you have provided your consent to the collection and use of your personal data; and
- Complain to the Information Commissioner's Office which is the supervisory authority for data protection in the UK.

Requests are normally free of charge and will be processed within one month of receipt. For complex or numerous requests we may extend the period by a further two months and will inform you accordingly. We may require proof of identity before fulfilling requests. You also have the right to complain to the ICO or, where applicable, to the supervisory authority in your country of residence.

DATA PRIVACY MANAGEMENT

We have appointed an internal team to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact us in the first instance: email: dataprotection@crownagentsbank.com; telephone: +44 (0)20 3903 3000.
If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact us in writing at: dataprotection@crownagentsbank.com, or Data Protection, Crown Agents Bank Limited, 3 London Bridge Street, London SE1 9SG.

BREACHES OF DATA PROTECTION PRINCIPLES

We hope that we can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at https://ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

If a personal data breach is likely to result in a high risk to your rights and freedoms we will notify you without undue delay and, where feasible, within 72 hours of becoming aware, including the nature of the breach, categories affected, and measures taken to mitigate harm.

CHANGES TO THIS PRIVACY NOTICE

This notice was last updated on 7th May 2026. We reserve the right to vary this notice from time to time by publishing a new version on our website.

SOURCES OF PERSONAL DATA

In addition to the information you provide on the Vendor Registration Form, we obtain personal data about you from public registers such as Companies House and sanctions lists, and from third party screening providers.

RECORD OF PROCESSING ACTIVITIES

We maintain a Record of Processing Activities in accordance with Article 30 GDPR, which is available to supervisory authorities upon request.