

EMpowerFX App - Privacy Notice

INTRODUCTION

This privacy notice describes how we will collect, use, share and otherwise process your personal data in connection with your use of:

- the EEmpowerFX mobile application (**App**) made available to Crown Agents Bank Limited clients (**CAB Clients, you or your**) to place instructions.
- Any services accessible through the App that enable CAB clients to create a login, set up a profile and place instructions (**Services**).

This App is not intended for children and we do not knowingly collect data relating to children.

Please read the following carefully to understand our practices regarding your personal data and how we will treat it.

Important information and who we are

Crown Agents Bank Limited (**CAB, we, us or our**) is the controller and is responsible for your personal data in connection with the App and Services.

CAB partners with Celer Technologies Limited (**Celer**) to make the App available to CAB clients. Celer supports the operation of the App on CAB's behalf so that authorised CAB clients can create a login, set up an entity profile and place instructions through the App.

We have appointed a data protection officer (**DPO**). If you have any questions about this privacy notice, please contact them using the details set out below.

Contact details

Our full details are:

- Full name of legal entity: Crown Agents Bank Limited
- Name or title of DPO: Shabana Uddin, Head of Enterprise Risk and UK DPO
- Email address: shabana.uddin@crownagentsbank.com
- Postal address: 3 London Bridge Street London SE1 9SG United Kingdom

As some of the CAB group is based outside of the UK, we have appointed Shabana Uddin as our UK and Edwin Weller as our EU representative under the UK GDPR and EU GDPR. You can contact them on the details below.

- Full name of legal entity: CAB Europe B.V
- Name or title of DPO: Edwin Weller, DPO EU
- Email address: edwin.weller@cabeurope.com
- Telephone number: +31 (0) 6 229 012 18

You have the right to make a complaint at any time to us, the Information Commissioner's Office (**ICO**), the UK regulator for data protection issues in line with our complaints procedure https://www.crownagentsbank.com/wp-content/uploads/2025/09/complaints_process.pdf

Changes to the privacy notice and your duty to inform us of changes

We keep our privacy notice under regular review.

This version was last updated on 9th September 2026. It may change and, if it does, those changes will be posted on this page and notified to you when you next log onto the App. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during our relationship with you.

Third party links and sites

Our App and Services may, from time to time, contain links to and from the websites of third parties. Please note that these websites (and any services accessible through them) are controlled by those third parties and are not covered by this privacy notice. You should review their own privacy notices to understand how they use your personal data before you submit any personal data to these websites or use these services.

The data we collect about you

We collect, use, store and transfer limited categories of personal data about you in connection with the App and Services. These categories are described in more detail in the section headed Description of categories of personal data.

- Identity Data.
- Contact Data.
- Profile Data.
- Entity Data.
- Security Data.
- Usage Data.

We do not collect any special categories of personal data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data).

We will collect data relating to criminal offences through the measures we take to secure and protect our App and users. Further details can be found at [Criminal offence data and special category data](#).

How is your personal data collected?

We collect your personal data in the following way:

- **Registration and account creation.** We collect your Identity Data, Contact Data, Profile Data and Security Data when an authorised CAB client creates a login for the App. This includes your first name, surname, email address or other selected authentication contact point, password and two-factor authentication preference.
- **Entity profile setup.** We collect Entity Data, such as company name and company or client identifier, to set up and maintain the App profile for the relevant CAB client entity.
- **Communications.** When you communicate with us via email, telephone, one of our online forms or chat we collect your Contact Data.
- **Information generated when using the App and Services.** Each time you access and use the App and Services, we may collect Usage Data, and Security Data needed to operate, monitor, troubleshoot and secure the App.
- **No marketing.** The App is not used for direct marketing and we do not collect Direct Marketing Data through the App.

How we use your personal data

We will only use your personal data when we have a lawful basis to do so. Our lawful basis for each purpose for which we use your personal data is specified below. Most commonly we will use your personal data in the following circumstances:

- **Consent.** Where you have freely consented before the processing in a specific, informed and unambiguous indication of what you want. You can withdraw your consent at any time by contacting us.
- **Performance of a contract.** Where we need to process your personal data to perform a contract with you or where you ask us to take steps before we enter into a contract with you. Where we rely on performance of a contract and you do not provide the necessary information, we will be unable to perform your contract.
- **Legitimate interests.** Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. You can obtain further

information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

- **Recognised legitimate interests.** We may sometimes use your personal data because we (or a third party) have a recognised legitimate interest (RLI). These are different to legitimate interests. RLIs apply where there are public interest reasons for processing (such as preventing or detecting crime, safeguarding individuals, responding to emergencies, supporting national or public security or defence, or sharing information with public bodies when they confirm it is necessary for their official functions). RLIs are legally recognised within data protection law. Where we rely on an RLI, we will ensure the use is strictly necessary and only use or share the minimum data required.
- **Legal obligation.** Where we need to use your personal data to comply with a legal or regulatory obligation. Where we rely on legal obligation and you do not provide the necessary information, we may be unable to fulfil a right you have or comply with our obligations to you, or we may need to take additional steps, such as informing law enforcement or a public authority or applying for a court order.

Delivery and improvement of our App and purchases

Purpose or activity	Type of personal data	Lawful basis for processing
To register you as an authorised App user and create your login	Identity Contact Profile Security	Performance of a contract and legitimate interests (delivering and securing the App and Services)
To enable CAB clients to set up an entity profile and place instructions through the App	Identity Contact Entity Usage	Performance of a contract and legitimate interests (providing the App and Services to CAB clients)

Troubleshooting, improvement and security

Purpose or activity	Type of personal data	Lawful basis for processing
To administer, monitor and improve our business, Services and this App including troubleshooting, data analysis and system testing	Identity Contact Device	Legitimate interests (for running our business, provision of administration and IT services, network security, maintaining the security of our App and Services, providing a secure service to users and preventing fraudulent and other misuse of our App)
Applying security measures to our processing of your personal data, including processing in connection with the App	All personal data under this privacy notice	Legal obligation (applying appropriate technical and organisational measures under Article 32 of the UK GDPR)
Otherwise monitoring use of the App and deploying appropriate security measures	Contact Security Transaction	Legitimate interests (running our business, provision of administration and IT services, network security, maintaining the security of our App and services, providing a secure service to users and preventing fraudulent and other misuse of our App)

Rights and obligations

Purpose or activity	Type of personal data	Lawful basis for processing
To comply with our other legal obligations, including compliance with tax legislation, judicial, law enforcement and government authorities' requests	All personal data under this privacy notice	Legal obligation — complying with applicable legal and regulatory obligations, including tax legislation, court orders, regulatory requirements and lawful requests from judicial, law enforcement or government authorities.

Other communications

Purpose or activity	Type of personal data	Lawful basis for processing
To notify you of changes to the App, Services, your purchases and our terms and conditions for ongoing contracts	Contact	For ongoing or prospective contracts, Performance of a contract
To notify you of updates to this privacy notice	Contact Transaction	Legal obligation to inform you of our processing under Articles 13 and 14 of the UK GDPR
To respond to your requests to exercise your rights under this notice	As relevant to your request	Legal obligation complying with data subject requests under Chapter 3 of the UK GDPR
To ask you to complete a survey and process your response (where applicable, please also see the separate privacy notice)	Contact	Legitimate interests to analyse how users use our products or Services and to develop them and grow our business) Unless you have previously opted out, where we will rely on Consent
To otherwise respond to your enquiries, fulfil your requests and to contact you where necessary	As relevant to your enquiry or request	Legitimate interests service our users and prospective users

Business contacts

Purpose or activity	Type of personal data	Lawful basis for processing
Process personal data relating to staff members of our business contacts, including suppliers, clients and prospects	Contact	Legitimate interests servicing and receiving products or services, to or from our business contacts and carry out our B2B business

Automated decision making and profiling

We do not make decisions based solely on automated processing or profiling that produce legal effects concerning you (or have similarly significant effects).

Criminal offence data and special category data

We do not intentionally collect criminal offence data about you. However, we may process data relating to criminal offences in monitoring the use of our App for security purposes, where we suspect you may have committed a crime, such as attempting to make a fraudulent purchase or claim or circumvent the

security of the App or Services. In such circumstances we will provide that information to law enforcement and/or use it to establish, exercise or defend a legal claim. In those circumstances, according to the type of activity and purpose, we will rely on legitimate interests (protecting our business, employees and other users) and legal obligation (where required by legal, judicial or law enforcement to disclose or process that information).

Special categories of personal data

We do not process the following special categories of personal data about you.

Disclosures of your personal data

We may share your personal data with the following third parties:

- **Internal third parties.** Other companies in the CAB group where necessary for governance, risk management, legal, regulatory, IT, security or system administration purposes.
- **External third parties.**
- Your Appstore Provider and mobile network operator to allow you to install the App.
- Celer, acting as a service provider in connection with the App, including hosting, data storage, operational support, authentication support and related technical services. Celer stores App data in a data centre.
- Your service providers that you have appointed and we need to contact to fulfil your requests, such as your banking or payment card provider to process your transactions.
- We do not share App personal data with marketing or promotional partners, and there are no fourth parties involved in the operation of the App.
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.
- HM Revenue and Customs, regulators, law enforcement, public authorities or other third parties based in the UK where necessary to exercise our rights or comply with a legal obligation.

International transfers

We do not transfer your personal data outside the EEA.

Data security

App data is stored in a data centre used to support the App. Where you create or are provided with a password to access the App or Services, you are responsible for keeping that password confidential and must not share it with anyone.

We may collect and store limited information on your device through standard cache browsing, and similar technologies required for App performance, security, authentication and operation.

We have put in place procedures to detect and respond to personal data breaches and notify you and any applicable regulator when we are legally required to do so.

Data retention

By law we have to keep basic information about our clients (including Contact, Identity, Security and Transaction Data) for six years after you cease being clients.

In some circumstances you can ask us to delete your data: see [Your legal rights](#) below for further information.

Once we no longer have a legal right to hold your personal data, we will delete or, in some circumstances, we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

Your legal rights

You have the following rights under data protection laws in relation to your personal data.

- **Access.** Request access to and/or a copy of the personal data we process about you (commonly known as a data subject access request). This enables you to check that we are lawfully processing it.

- **Correction.** Request correction of any incomplete or inaccurate data we hold about you. (We may need to verify the accuracy of the new data you provide to us.)
- **Deletion.** Request us to delete or remove personal data where there is no good reason for us continuing to process it. You also can ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we have processed your information unlawfully or where we need to erase your personal data to comply with law. (In some cases, we may need to continue to retain some of your personal data where required by law. If these apply, we will notify you at the time of our response)
- **Objection.** Object to us processing your personal data where (a) we are relying on legitimate interests as the lawful basis and you feel the processing impacts on your fundamental rights and freedoms, or (b) the processing is for direct marketing purposes. In some cases, we may refuse your objection if we can demonstrate that we have compelling legitimate grounds to continue processing your information which override your rights and freedoms.
- **Restriction.** Request that we restrict or suspend our processing of your personal data:
 - if you want us to establish the data's accuracy;
 - where our use of the data is unlawful, but you do not want us to erase it;
 - where we no longer require it, but you need us to hold onto it to establish, exercise or defend legal claims; or
 - you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.
- **Data portability.** Request we transfer certain of your personal data to you or your chosen third party in a structured, commonly used, machine-readable format. This right only applies to information processed by automated means that we process on the lawful bases of consent or performance of a contract.
- **Withdraw consent.** Withdraw your consent at any time where we are relying on consent to process your personal data. Please know that this does not affect the lawfulness of any processing carried out before you withdraw your consent, and after withdrawal, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent
- **Complain to us.** If you are unhappy with how we process your personal data, please contact us first using the details below so that we have the chance to put it right. Under the UK GDPR, you may also have the right to make a complaint to us, which can be made via your Relationship Banker. We will deal with all complaints in line with our complaints procedure, including to keep you informed about the progress and outcome of your complaint.
- **Complain to the UK data protection regulator.** If you are unhappy with how we process your personal data, we ask that you contact us first, as described above so that we have the chance to put it right. However, you also have the right to make a complaint to the ICO at any time.

You can exercise any of these rights at any time by contacting the DPO.

Description of categories of personal data

- **Identity Data:** first name and surname.
- **Contact Data:** email address, mobile number and any other contact details used to support account access, authentication or App communications.
- **Profile Data:** username, password, App profile details and selected authentication method.
- **Entity Data:** company name, company or client identifier and other details needed to set up or maintain the CAB client entity profile in the App.
- **Device Data:** IP address.
- **Usage Data:** logs and detail of your use of our Apps and Services, being the dates and times on which you download, access and update the App and our Services, any error or debugging information.
- **Security Data:** information we collect about your use of the App, our Services and our Sites in order to ensure your and our other users' safety and security, being Usage Data, and the information provided to us by our payment processing provider.