Privacy Policy

Co-operative Brokerage Finance Limited

Website: https://cubfinance.co.uk/

Email: james@cubfinance.co.uk

Introduction

This is the privacy policy for Co-operative Brokerage Finance Limited

Referred to as “we”, “us” or “our” in this policy), our website https://cubfinance.co.uk/ and any associated applications or services (“our services”).

Co-operative Brokerage Finance Limited respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from), apply for or use our products and services, and tell you about your privacy rights and how the law protects you.

Co-operative Brokerage Finance Limited acts as the **Data Processor** of the personal data we collect and process in relation to applications we process on behalf of our Member Credit Unions and users of our services.

This privacy policy relates to personal data collected directly by us and data obtained from third parties in connection with providing our services, including credit reference agencies, fraud prevention agencies and Open Banking providers.

Co-operative Brokerage Finance Limited is a registered Co-operative in the United Kingdom and is registered with:

- **FCA Mutuals Register** (Registration No. 5468)
- Information Commissioner’s Office (ICO) (Registration No. ZC065492)

This Privacy Policy (together with our Cookie Policy, Terms and Conditions, and any product-specific terms) sets out the basis upon which we will process personal information that:

- is collected from you when you use our website or services;

- is collected when you apply for, or express an interest in, a product or service processed by us;

- we receive from third parties in order to assess applications, verify identity, prevent fraud, and meet our legal and regulatory obligations.

Please read this Privacy Policy carefully, as it contains important information to help you understand how we collect, use and protect your personal data.

By accessing, browsing or otherwise using our website or services, or by applying for products processed by us, you confirm that you have read and understood this Privacy Policy. If you do not agree with any part of this Privacy Policy, you should not use our services or provide your personal data.

It is important that you read this privacy policy together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data.

Role of CUB and Partner Credit Unions

We operate as a **technology and application processing platform** that enables Credit Unions to receive, assess and manage finance applications.

We do not provide loans directly. All lending decisions are made by the relevant Credit Union in accordance with their own credit policies

1. Information We Collect

Personal Data

We may collect personal information (which means any information about an individual whose identity is apparent or can be reasonably ascertained from such information) from you in connection with a product or service processed by us.

This may include:

- **Identity Data**: Including first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, gender, and proof of identity (including photographs or “selfies” to confirm that identification documents relate to you, and copies of or details from identification documents such as your passport or driving licence).

- **Contact Data**: Including billing address, residential address, email address and telephone numbers.
- **Employment and Income Data**: Including current and previous employers, nature of employment, occupation, place of work, commuting details where relevant, income, and proof of income.
- **Expenditure Data**: Including current and expected outgoings, including financial commitments and dependants.
- **Credit Data**: Including your credit history, credit score, repayment behaviour and publicly available information such as County Court Judgments (CCJs), bankruptcies, insolvencies or repossessions.
- **Bank Account Data**: Including bank account details and transactional data, including where this is obtained via Open Banking (with your consent).
- **Credit Card Data**: Including card details where required to facilitate payments.
- **Insurance Data**: Including details of any insurance policies held in connection with a product or service and any associated claims history (where applicable).
- **Technical Data**: Including internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access our website or services.
- **Transaction Data**: Including details about payments to and from you, savings contributions, loan repayments, and other details of agreements you have or have had with us.
- **Profile Data**: Including your username and password, account preferences, feedback, and responses to surveys.
- **Usage Data**: Including information about how you use our website, products and services.
- **Marketing and Communications Data**: Including your preferences in receiving marketing from us and your communication preferences.
- **Survey Data**: Including responses to surveys carried out by us or by authorised third parties on our behalf.
- **Video Footage**: Including CCTV footage captured on our premises and recordings of meetings or calls where appropriate and with your knowledge.

  Special Category (Sensitive) Data: Including information relating to your health or personal circumstances where you choose to provide this (for example, where this is relevant to assessing affordability or providing appropriate support). Further details are set out in the “Sensitive Personal Data” section below.

Mandatory Information

Where information fields are marked as mandatory on any form, you will need to provide this information in order for us to process your application or provide the requested service.

Where you begin an application but do not complete it, we may use the information you have provided to contact you in order to support you in completing the application or to clarify your requirements.

Failure to Provide Personal Data

Where we are required to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to process the contract or provide the product or service requested.

In such cases, we may have to decline or cancel the relevant service or application, but we will notify you if this is the case.

Aggregated Data

We also collect, use and share aggregated data such as statistical or demographic data.

Aggregated data may be derived from your personal data but is not considered personal data in law where it does not directly or indirectly identify you. For example, we may aggregate usage data to understand how members use our services.

However, where aggregated data is combined with personal data so that you can be identified, it will be treated as personal data and handled in accordance with this privacy policy.

Third-party Links

This website/application may include links to third-party websites, plug-ins and applications, such as social media links. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

2. How We Collect Data

We use different methods to collect data from and about you, including through:

Direct Interactions

You may provide us with your Identity, Contact, Financial and other personal data by filling in forms or by corresponding with us through online platforms, such as ClearScore and Jigsaw

This includes personal data you provide when you:

- apply for any loan or other financial product or service processed by us;
- subscribe to our services, communications or publications;
- provide information to us via our website, mobile applications, in writing, through social media, or over the phone (including where calls may be recorded for training, monitoring and compliance purposes);
- register an interest in a product, service or employment opportunity;
- request information, support or assistance from us;
- enter a competition, promotion or survey;
- make a complaint or raise a query; or

  provide feedback or otherwise contact us.

Automated Technologies or Interactions

As you interact with our website or digital services, we will automatically collect Technical Data about your equipment, browsing actions and usage patterns.

We collect this personal data using cookies, server logs and other similar technologies. This may include tracking your use of our website, pages visited, time spent on pages and interactions with our services.

We may also receive Technical Data about you if you visit other websites that use our cookies or similar technologies.

Further details can be found in our Cookie Policy on our website.

Third Parties and Publicly Available Sources

We may receive personal data about you from a range of third parties and public sources where this is necessary to provide our services, assess applications, verify identity, prevent fraud and meet legal and regulatory obligations.

This includes:

Technical Data

- Analytics providers (such as Google), which may be based outside the UK
- Search information providers

Contact, Financial and Transaction Data

- Providers of technical, payment and delivery services
- Open Banking providers (such as **Data One**), where you have given consent for us to access your bank account information

Identity and Contact Data

- Publicly available sources (such as the electoral register)
- Driving licence and identity verification service providers

Credit and Financial Data

- Credit Reference Agencies (including **TransUnion**) who provide credit reports, credit scores and financial history data
- Open Banking account information providers (with your consent)

Fraud Prevention and AML Data

- Identity verification providers
- Anti-fraud and anti-money laundering agencies
- Organisations providing fraud prevention, sanctions screening and politically exposed person (PEP) checks

This combination of sources allows us to:

- verify your identity;
- assess your creditworthiness and affordability;
- prevent fraud and financial crime; and
- ensure that any products or services offered are appropriate to your circumstances.

3. Lawful Basis

We will only use your personal data where the law allows us to do so. Most commonly, we will use your personal data in the following circumstances:

- where we need to process an application for you on behalf of our member Credit Unions;
- where it is necessary for our legitimate interests (or those of a third party), provided your interests and fundamental rights do not override those interests;
- where we need to comply with a legal or regulatory obligation; and
- where you have provided your consent to specific processing activities.

The lawful bases on which we collect, use and process your personal data can therefore be broadly defined as:

- Consent
- Contractual necessity
- Legal obligation
- Legitimate interests

We may rely on more than one lawful basis depending on the specific purpose for which we are using your data. If you require further details about the specific legal basis we are relying on for a particular processing activity, please contact us.

Consent

Where we rely on your consent, we will ensure that it is freely given, specific, informed and unambiguous.

We may rely on consent for activities including, but not limited to:

- accessing your bank account information via **Open Banking providers (such as Data One)** to assess affordability and verify financial information;
- sending you marketing communications by email, SMS or other electronic means;
- carrying out certain optional checks or services where consent is required by law;
- recording calls or meetings where this is not otherwise justified under another lawful basis;
- processing certain categories of sensitive personal data where applicable.

Where you have provided consent, you have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of processing carried out prior to withdrawal, but may affect our ability to provide certain products or services.

We will always seek your consent before sending direct marketing communications from third parties. You can withdraw your consent to marketing at any time by contacting us or using the unsubscribe options provided.

Contractual Necessity

We process personal data where it is necessary to process an application from you on behalf of our member Credit Unions.

In the context of our services as a credit union service organisation, this includes activities such as:

- processing applications for loan products
- gathering and assessing financial information to determine **creditworthiness and affordability**;
- verifying your identity and eligibility to hold an account or receive a loan;
- ensuring that you are able to meet repayment obligations under any agreement;
- administering and enforcing the terms of any agreement between you and us.

Without this processing, we would not be able to provide the services you have requested.

Legal and Regulatory Obligations

We process personal data where it is necessary to comply with our legal and regulatory obligations as a credit union and FCA-regulated firm.

These obligations include, but are not limited to:

- compliance with anti-money laundering (AML), counter-terrorist financing (CTF) and know your customer (KYC) requirements;
- identity verification and sanctions screening, including checks against politically exposed persons (PEP) lists;
- fraud detection, prevention and reporting, including sharing data with fraud prevention agencies and law enforcement bodies;
- reporting and oversight requirements imposed by regulators such as the **Financial Conduct Authority (FCA)**;
- compliance with data protection laws and oversight by the **Information Commissioner's Office (ICO)**;
- maintaining appropriate records for regulatory, audit, tax and accounting purposes;
- responding to lawful requests from courts, regulators or law enforcement agencies.

Where required, we may share your data with relevant authorities and agencies in order to meet these obligations.

Legitimate Interests

We may process your personal data where it is necessary for our legitimate interests (or those of a third party), provided those interests are not overridden by your rights and freedoms.

Our legitimate interests include:

- managing risk within our lending activities, including credit risk assessment and account monitoring
- preventing fraud, financial crime and misuse of our services;
- improving and developing our products, services and member experience;
- conducting analytics, research and statistical analysis (typically using anonymised or pseudonymised data where possible);
- ensuring our systems, processes and controls operate effectively and securely;
- supporting business operations, including internal reporting, training and quality assurance;
- protecting our business, members and staff from financial loss or harm.

Where we rely on legitimate interests, we ensure that:

- the processing is necessary for the stated purpose;
- we have considered the impact on your rights and freedoms; and
- appropriate safeguards are in place, including minimisation and, where appropriate, pseudonymisation of data.

We will not use personal data collected under legitimate interests for direct marketing where you have opted out of such communications.

4. Use of Data

Your personal data will be used by us in connection with the following purposes:

Service / Product Provision and Internal Processing

This means where we need to use your personal data:

- to assess and process your application for membership, savings accounts, loans or related services of our member Credit Unions;
- to enable our trusted partners, to provide you with products or services suited to your needs;
- to evaluate risk in connection with the provision of products and services, including **credit risk, affordability assessment and lending decisions** (please see

the section on Credit Checking and Automated Decision Making for further detail);
- to provide quotations and assess eligibility for products or services;
- to troubleshoot issues with our website, systems or services and to improve your experience;
- to administer promotions, competitions or member initiatives where applicable;
- to personalise your experience and interactions with us;

Handling Queries, Requests and Complaints

This means where we need to use your personal data:

- to respond to queries, requests or complaints you raise;
- to contact you where there are service updates, operational issues, or changes affecting your application;
- to contact you where an application or form has been started but not completed;
- to investigate and resolve any issues relating to the accounts, services or products provided by us or one of the credit unions we are working on behalf of.

Training, Service Review and Statistical Analysis

This means where we need to use your personal data:

- for staff training, monitoring and quality assurance purposes;
- to review, develop and improve our products, services and internal processes;
- to carry out statistical analysis and research to better understand member needs and behaviours;
- to improve our website, communications, and overall member experience.

Where possible, this analysis will be carried out using anonymised data.

To Verify Your Identity and Prevent Fraud or Money Laundering

This means where we need to use your personal data:

- to carry out identity verification checks before providing products or services;
- to confirm the accuracy of the information you provide;
- to prevent, detect and investigate fraud, financial crime and misuse of our services;
- to comply with anti-money laundering (AML), counter-terrorist financing (CTF) and know your customer (KYC) requirements.

Legal and Regulatory Obligations

This means that we or the credit unions that use our services, may need to use your personal data:

- to prevent, investigate and prosecute fraud, financial crime and other unlawful activity;
- to comply with legal obligations, regulatory requirements or court orders;
- to share data with regulators, law enforcement agencies or fraud prevention agencies where required;
- to comply with obligations relating to sanctions screening and politically exposed persons (PEP) checks;
- where we, the credit unions that use our services, or fraud prevention agencies, determine that you pose a fraud or money laundering risk, we may refuse to provide the products or services requested, or we may suspend or terminate existing services.

A record of any fraud or money laundering risk may be retained by fraud prevention agencies and may result in other organisations refusing to provide services, financing or employment to you.

General Use of Data for Fraud Prevention and Risk Management

This means where:

- personal data provided by you, collected from you, or obtained from third parties is used to prevent fraud, money laundering and to verify identity;
- we, the credit unions that use our services and fraud prevention agencies may share and access personal data to detect, investigate and prevent crime;
- we or the credit unions that use our services process your personal data on the basis of legitimate interests in protecting our members, our organisation and the wider financial system;
- such processing is also a requirement of our lending partners providing financial services and entering into agreements with you;
- fraud prevention agencies may retain your personal data for varying periods of time and, where a risk is identified, may retain such data for up to six years.

Other Uses

We may also:

- transfer your personal data to any entity that acquires rights in us as part of a business restructure, merger or transfer;

- use your personal data for any other purpose where you have provided your consent.

Opting Out of Marketing

You can ask us (or third parties where applicable) to stop sending you marketing messages at any time by:

- following the opt-out links included in any marketing communications; or
- contacting us directly using the contact details provided.

Please note that opting out of marketing communications will not affect communications that are necessary for the administration of your account or the provision of services.

5. How We May Share Your Information

We may share your personal data with the following categories of third parties where it is necessary to provide our services, meet our legal and regulatory obligations, manage risk, or support our business operations:

Group Companies and Affiliates

- Our subsidiaries, affiliates or partner organisations (where applicable), for the purposes of managing member relationships, administering our business and, where appropriate, providing information about relevant products and services.

Insurance Providers (Where Applicable)

- Insurance providers with whom we work, where insurance products are offered in connection with our services, in order to process applications, administer policies, and manage claims or potential claims.
- Insurance providers with whom we use for insurance services as a company, in order to administer policies, and manage claims or potential claims

Credit Reference Agencies and Fraud Prevention Agencies

- Credit Reference Agencies, including **TransUnion**, who provide credit reports, credit scores and financial history data to support decision-making;
- Fraud prevention agencies and organisations involved in the detection and prevention of financial crime, which may include CIFAS or similar bodies;

These organisations may:

- receive and process your personal data;
- retain records of searches and outcomes;
- share data with other organisations;

Further information is provided in the section on Credit Checking and Automated Decision Making, including reference to the Credit Reference Agency Information Notice (CRAIN).

Open Banking Providers

- Open Banking providers (such as **Data One**) who, with your explicit consent, provide access to your bank account information to support affordability assessments, identity verification and payment services;

This may include:

- assessing your financial position;
- verifying income and expenditure;
- facilitating secure account-to-account payments.

Service Providers and Operational Partners

- Third-party service providers who process personal data on our behalf to support the operation of our business, including:
    - payment processing providers;
    - IT and system providers;
    - data storage and document management providers;
    - electronic signature and onboarding platforms;
    - communications providers (e.g. email, SMS);
    - customer support and administration services;
    - analytics and reporting providers (typically using anonymised or pseudonymised data where possible).

All such providers are subject to contractual obligations to protect your personal data.

Regulators and Law Enforcement

- Regulatory bodies such as the Financial Conduct Authority (FCA) and the Information Commissioner's Office (ICO);

- Law enforcement agencies, courts, or other authorities where disclosure is required by law or necessary for the prevention or detection of crime.

Third-Party Lenders or Partners

- Where your application is unsuccessful with us, and where appropriate and permitted, we may introduce or refer you to third-party providers who may offer suitable products or services.

In such cases:

- your data will only be shared where lawful to do so;
- the third party will become the **data controller** of your information and will provide their own privacy policy.

Professional Advisors and Business Support

- Professional advisors, including auditors, legal advisors, consultants and other specialists who support us in operating and developing our business and ensuring compliance with legal and regulatory requirements.

Business Transfers and Reorganisation

- Third parties who acquire, or may acquire, rights in us as part of a business sale, merger, restructuring or other corporate transaction.

Recruitment and Employment (Where Applicable)

- Third parties involved in assessing suitability for employment where you apply for a role with us.

Marketing Partners (Where You Have Consented)

- Selected third parties where you have agreed to receive marketing communications relating to relevant products or services.

Applications via Third Parties

If you apply for a product or service through a third party (for example, an introducer or broker), we and the credit unions that use our services may:

- use your personal data to assess your circumstances;
- verify the information provided;

- carry out credit, affordability and identity checks before providing a decision.

6. Credit Checking and Automated Decision Making

Whenever you apply for a product or service through our platform, we will process your application on behalf of one or more partner Credit Unions.

As part of this process, we and/or relevant third parties may carry out **automated, manual, or partially automated assessments** using rules and criteria defined by the relevant Credit Union(s). These assessments are used to support the evaluation of your application and ongoing suitability for financial products.

Initial decisioning may be carried out through our platform using automated systems; however, **final lending decisions are made by the relevant Credit Union**, and applications may be subject to automated or manual review where appropriate

This may include checks with **Credit Reference Agencies ("CRAs")**, Open Banking providers, fraud prevention agencies and other relevant data sources.

Credit Reference Agency Checks

As part of our assessment processes, we and the credit unions that use our services may carry out checks with CRAs (including **TransUnion**), which may include:

- Credit application searches ("hard searches")

These involve checks against your financial history and current financial position and may be visible to other lenders and organisations.

- Quotation searches ("soft searches")

These involve checks against publicly available information such as the Electoral Register, County Court Judgments (CCJs), bankruptcy or repossession data. These searches are typically only visible to you.

Use of Open Banking Data

We and the credit unions that use our services may also request access to your current account information via a regulated Open Banking provider (such as **Data One**) or, alternatively, request bank statements directly from you.

Where Open Banking is used:

- you will be securely redirected to your bank or financial provider;

- you will authenticate directly with your provider using their own secure systems;
- we will never have access to your login credentials or security details;
- we will only access the specific accounts and information you choose to share.

Types of Open Banking Data Collected

With your consent, we may collect and analyse information including:

- your income and sources of income;
- transaction data, including spending patterns and behaviours;
- regular commitments and outgoings;
- account balances and financial position;
- details of missed payments, fees, charges, interest or arrears;
- payment data where you choose to make or receive payments via Open Banking.

How We Use Credit and Open Banking Data

We and the credit unions that use our services use information obtained from CRAs and Open Banking to:

- assess your creditworthiness and affordability;
- determine whether you can sustainably meet repayments;
- verify the accuracy of the information you have provided;
- support identity verification processes;
- prevent and detect fraud, financial crime and money laundering;
- manage your account(s) and ongoing relationship with us;
- trace and recover outstanding debts;
- ensure that any products or services offered to you are appropriate to your circumstances.

Open Banking Consent and 90-Day Access Window

Access to your account information via Open Banking is strictly controlled and based on your explicit consent.

- When you provide consent, we and the credit unions that use our services may access your account data for a period of up to **90 days**;
- Before the end of this period, if we and the credit unions that use our services require continued access, we will request that you **reconfirm your consent (repermissioning)**;
- If you provide renewed consent, access may continue for a further 90-day period;

- If you do not provide renewed consent, or withdraw your consent, our access and that of the credit unions that use our services to your Open Banking data will automatically cease.

You can withdraw your consent at any time through your bank or by contacting us.

Impact of Withdrawing Open Banking Consent

If you choose not to provide, or withdraw, Open Banking access:

- we and the credit unions that use our services may not be able to fully assess your affordability or financial circumstances;
- this may affect our ability to offer certain products or services;
- in some cases, we and the credit unions that use our services may be unable to proceed with an application or may need to review existing products to ensure they remain appropriate.

Ongoing Data Sharing with Credit Reference Agencies

We and the credit unions that use our services will continue to exchange information about you with CRAs while you have a relationship with us or them.

This includes:

- sharing details of your account performance;
- reporting when accounts are settled;
- reporting missed or late payments and outstanding debts.

CRAs may:

- retain this information;
- share it with other organisations;
- use it to support lending and fraud prevention decisions across the financial services sector.

When CRAs receive a search request from us, they will place a record (“footprint”) on your credit file.

Financial Associations

If you apply jointly with another individual, or indicate that you have a financial associate (such as a spouse or partner):

- your financial records may be linked;

- CRA records may reflect this association;
- these links will remain until a formal disassociation request is made and accepted by the relevant CRA.

You should ensure that you have the consent of any joint applicant or associate before providing their information.

Credit Reference Agency Information Notice (CRAIN)

Detailed information about how CRAs collect, use, share and retain personal data, and your rights in relation to this, is set out in the **Credit Reference Agency Information Notice (CRAIN)**.

You can access this here:

👉 https://www.transunion.co.uk/crain

Additional information is also available from other CRAs, including Equifax and Experian.

Fraud Prevention Agencies and International Transfers

Fraud prevention agencies may share and transfer your personal data, including outside the UK or the European Economic Area.

Where this occurs, appropriate safeguards are applied, including:

- contractual protections;
- adherence to recognised international data protection frameworks;

to ensure your personal data remains protected.

Automated Decision Making and Your Rights

Credit scoring and affordability assessments may involve automated decision-making.

However:

- decisions are typically supported by manual review where appropriate;
- you have the right to request **human intervention**;
- you may ask us to review, reconsider or explain any decision made about you.

If a decision is made solely using automated processing and has a significant effect on you (such as declining a loan), you have the right to challenge that decision.

8. Data Security

We take the security of your personal data seriously and invest appropriate technical and organisational measures to protect it from loss, misuse, unauthorised access, alteration or disclosure.

In particular:

We regularly review our information collection, storage and processing practices, including physical, electronic and procedural safeguards, to protect against unauthorised access to our systems and data;

We implement appropriate security measures, which may include encryption, secure networks, access controls and system monitoring, to ensure the confidentiality, integrity and availability of your personal data;

Access to personal data is strictly limited to employees, contractors, service providers and agents who have a legitimate business need to access it in order to perform their duties. All such individuals are subject to strict confidentiality obligations and appropriate training in data protection;

We ensure that third-party service providers who process personal data on our behalf are subject to contractual obligations to implement appropriate security measures and to protect your data in line with applicable data protection laws;

We maintain internal policies and procedures designed to safeguard personal data and ensure compliance with legal and regulatory requirements, including those set by the Financial Conduct Authority (FCA) and the Information Commissioner's Office (ICO);

We have established procedures to detect, investigate and respond to suspected personal data breaches. Where a breach is likely to result in a risk to your rights and freedoms, we will notify you and the relevant regulator where we are legally required to do so;

We regularly review and test our security measures to ensure they remain effective and appropriate to the nature of the data we process.

9. Retention of Your Personal Information

We will only retain your personal data for as long as is reasonably necessary to fulfil the purposes for which it was collected, including to meet applicable legal, regulatory, tax, accounting and reporting requirements.

Where we process personal data on behalf of our partner Credit Unions, we will retain and handle that data in accordance with their instructions and applicable regulatory requirements.

This includes retaining data to:

• support the assessment and processing of applications on behalf of Credit Unions;

• enable responsible lending, account administration and ongoing customer management by the relevant Credit Union;

• comply with anti-money laundering, fraud prevention and financial crime requirements; and

• meet our obligations as a credit union service organisation and technology provider.

We may retain personal data for longer periods where:

• a complaint has been raised;

• there is a reasonable prospect of litigation;

• we are required to do so by law, regulation or regulatory guidance; or

• it is necessary for the establishment, exercise or defence of legal claims.

How We Determine Retention Periods

In determining appropriate retention periods, we consider:

• the nature, sensitivity and volume of the personal data;

• the potential risk of harm from unauthorised use or disclosure;

• the purposes for which we process the data and whether those purposes can be achieved by other means;

• whether we are acting on our own behalf or on behalf of a Credit Union; and

• applicable legal, regulatory and industry requirements, including FCA expectations and financial crime obligations.

Regulatory Retention Requirements

As part of our role supporting regulated financial services, certain data must be retained for defined periods.

In particular:

• where we process data on behalf of Credit Unions, core applicant and customer data (including Identity, Contact, Financial and Transaction Data) will typically be retained for a minimum of six years after the end of the customer's relationship with the relevant Credit Union, in line with legal, regulatory and tax requirements;

• information relating to credit agreements, account performance, arrears and collections activity may be retained for similar or longer periods where required by the relevant Credit Union for regulatory, audit or risk management purposes;

• data shared with Credit Reference Agencies may continue to be held and used by those agencies in accordance with their own retention policies and the Credit Reference Agency Information Notice (CRAIN).

Where we and the credit unions that use our services hold personal data for our/their own operational purposes (such as platform management, analytics, or compliance), retention periods may differ and will be limited to what is necessary for those purposes.

Fraud Prevention and Financial Crime Data

Where personal data is processed for the purposes of fraud prevention, anti-money laundering or financial crime detection:

- such data may be retained for extended periods where required by law or fraud prevention agencies;
- in some cases, this may be up to **six years or longer**, depending on the nature of the risk identified;

- this information may continue to be used by fraud prevention agencies and shared with other organisations to prevent financial crime.

Your Right to Request Deletion

In certain circumstances, you have the right to request that we delete your personal data (also known as the **"right to be forgotten"**).

However, this right is not absolute. We may retain your data where it is necessary to:

- comply with legal or regulatory obligations;
- fulfil contractual requirements;
- prevent fraud or financial crime;
- establish, exercise or defend legal claims.

Further details are set out in the **Your Rights & Freedoms** section of this policy.

Anonymisation

In some circumstances, we may anonymise your personal data so that it can no longer be associated with you.

Where data has been fully anonymised (so that you can no longer be identified), we may use this information indefinitely for:

- statistical analysis;
- research and development;
- improving our products, services and risk models;

without further notice to you.

10. International Transfers

We and the third parties who process your personal data on our behalf may, from time to time, transfer or store your personal data outside of the United Kingdom.

This may occur where:

- we use service providers who operate internationally (for example, IT systems, cloud storage or data processing services);

- data is processed by Credit Reference Agencies, fraud prevention agencies or Open Banking providers that operate across multiple jurisdictions;
- it is necessary to support the delivery of our services or the operation of our business.

Safeguards for International Transfers

Where personal data is transferred outside of the UK, we ensure that appropriate safeguards are in place to protect your data and ensure that it continues to be handled securely and in accordance with applicable data protection laws.

These safeguards may include:

- transferring data only to countries that have been deemed by the UK Government to provide an **adequate level of protection** for personal data;
- putting in place **UK-approved contractual safeguards**, such as the UK International Data Transfer Agreement (IDTA) or Standard Contractual Clauses, which require recipients to protect personal data to UK standards;
- ensuring that service providers and partners implement appropriate technical and organisational security measures;
- carrying out due diligence and, where appropriate, risk assessments in relation to international data transfers.

Further information on international transfers is available from the Information Commissioner's Office (ICO):

👉 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

Your Rights and Protections

Where your personal data is transferred internationally:

- we will take all reasonable steps to ensure that your data is treated securely and in accordance with this privacy policy;
- you retain all rights granted to you under UK data protection law;
- you may contact us if you would like further information about the safeguards we have in place.

11. Special Category (Sensitive) Personal Data

Certain types of personal data are considered more sensitive under data protection law and require a higher level of protection. This includes information relating to:

- your health or medical conditions;
- criminal convictions or offences;
- and other categories defined as “special category data” under UK GDPR.

We and the credit unions that use our services do not generally seek to collect or process special category personal data.

However, we and the credit unions that use our services may process such data where:

- you have voluntarily provided it to us (for example, where you inform us of a health condition or personal circumstance);
- it is necessary to provide our services appropriately, including where this supports affordability assessments, vulnerability considerations or forbearance;
- it is required for compliance with legal or regulatory obligations; or
- we are otherwise permitted to do so under applicable data protection laws.

How We Use Sensitive Data

Where special category data is processed, we will only use it where necessary and proportionate, including for purposes such as:

- ensuring that products and services are appropriate to your circumstances;
- identifying and supporting **vulnerable applicants**, including where health or personal circumstances may impact financial wellbeing;
- providing appropriate assistance where you experience financial difficulty;
- meeting legal and regulatory requirements.

Lawful Basis and Safeguards

Where we process special category personal data, we will do so in accordance with UK GDPR, relying on:

- your **explicit consent**, where required; and/or
- other lawful bases permitted under data protection law (such as substantial public interest or legal obligations).

We will ensure that:

- access to such data is strictly limited;
- additional security measures are applied where appropriate;
- data is only retained for as long as necessary.

Data Minimisation

We are committed to **minimising the collection and use of sensitive personal data**. We will only collect such information where it is necessary for the purposes described above and will not use it for unrelated purposes.

12. Marketing

Where you have indicated that you are happy to receive information from us, we may send you communications about products and services that we believe may be of interest to you.

This may include:

- information about savings accounts, loan products and related services offered by us;
- updates about new or enhanced products and services;
- information about relevant products or services offered by selected partners, where you have agreed to receive such communications.

How We Contact You

Depending on your preferences, we may contact you by:

- post;
- telephone;
- email;
- SMS; or
- other electronic means, including online and social media platforms where appropriate.

All marketing communications will be carried out in accordance with applicable laws, including the **Privacy and Electronic Communications Regulations (PECR)**.

Your Choices and Preferences

You are in control of how we use your data for marketing purposes.

You can:

- choose whether or not to receive marketing communications when you first provide your details;
- update your preferences at any time;
- opt out of receiving marketing communications entirely.

Opting Out

You can ask us to stop sending you marketing communications at any time by:

- clicking the “unsubscribe” link included in any marketing email;
- contacting us using the details provided in this policy; or
- updating your communication preferences where this option is available.

We will process your request as soon as reasonably practicable.

Important Information

Please note that opting out of marketing communications will not affect:

- service-related communications that are necessary for the administration of your account;
- important updates about products or services you hold with us or the credit unions that use our services;
- communications required to meet our legal or regulatory obligations.

13. Third-Party Websites

This Privacy Policy applies only to personal data collected and processed by us.

Our website and services may contain links to third-party websites, applications or services. These third parties may operate independently from us and have their own privacy policies and practices.

We do not control, and are not responsible for, the content, security or data handling practices of third-party websites or services. This includes organisations that may advertise our services or use technologies such as cookies, pixel tags or similar tools to deliver targeted advertising.

When you leave our website or access third-party services, we encourage you to read the privacy policy of each website or service you visit.

14. Email Communications

Communications sent over the internet, including email, are not always secure and may be subject to interception, loss, delay or alteration.

While we take appropriate steps to protect your personal data, we cannot guarantee the security of information transmitted to us via email. Any information you send to us electronically is therefore done at your own risk.

Where possible, we encourage you to avoid sending sensitive personal or financial information via unsecured email channels. If you need to contact us regarding sensitive matters, please use the contact methods provided in this policy or on our website.

We will take reasonable steps to protect any personal data received and handle it in accordance with this Privacy Policy.

15. Cookies

Our website uses cookies and similar technologies to distinguish you from other users and to improve your experience.

These may include:

- essential cookies required for the operation of our website;
- performance and analytics cookies (such as Google Analytics) to help us understand how visitors use our website;
- functionality cookies to enhance your experience;

16. Your Rights & Freedoms

Under UK data protection law, you have a number of important rights in relation to your personal data.

Right to Be Informed

You have the right to be provided with clear, transparent information about how your personal data is collected and used. This Privacy Policy forms part of how we meet that obligation.

Right of Access

You have the right to request access to the personal data we hold about you (commonly known as a “subject access request”).

We will normally respond within **one month**, and this is usually free of charge. We may extend this period where requests are complex or numerous, in line with legal requirements.

Right to Rectification

You have the right to request that inaccurate or incomplete personal data is corrected.

We will take reasonable steps to update your information promptly once we have verified your identity and the accuracy of the request.

Right to Restrict Processing

You have the right to request that we restrict the processing of your personal data in certain circumstances, for example where you contest the accuracy of the data or object to its use.

Right to Object

You have the right to object to the processing of your personal data where we rely on legitimate interests.

You also have the absolute right to object to the use of your personal data for **direct marketing purposes**, and we will act on such requests promptly.

Right to Erasure (Right to be Forgotten)

You have the right to request that we delete your personal data in certain circumstances.

However, this right is not absolute. We and the credit unions that use our services may retain your data where it is necessary to:

- comply with legal or regulatory obligations;
- fulfil contractual requirements;
- prevent fraud or financial crime;
- establish, exercise or defend legal claims.

We will assess each request carefully and inform you of the outcome.

Right to Data Portability

You have the right to receive the personal data you have provided to us in a structured, commonly used and machine-readable format and, where technically feasible, to have that data transmitted to another organisation.

Rights Relating to Automated Decision-Making

You have rights in relation to decisions made solely by automated means that have a legal or similarly significant effect on you.

These include the right to:

- request human intervention;
- express your point of view;
- challenge or request a review of the decision.

Further details are set out in the Credit Checking and Automated Decision Making section.

Exercising Your Rights

You can exercise your rights by contacting us using the details provided in this policy.

We may need to request specific information from you to verify your identity before responding to your request. This is to ensure that personal data is not disclosed to unauthorised individuals.

You will not usually be required to pay a fee. However, we may charge a reasonable fee or refuse to comply where a request is clearly unfounded, repetitive or excessive.

We aim to respond to all legitimate requests within **one month**, although this may be extended where necessary. If an extension is required, we will notify you.

17. Complaints Process

If you have any concerns about how we have handled your personal data, please contact us in the first instance and we will investigate your complaint.

We aim to resolve complaints promptly and fairly.

You also have the right to lodge a complaint with the **Information Commissioner's Office (ICO)**, the UK supervisory authority for data protection matters:

👉 https://ico.org.uk

18. Updates To This Policy

This Privacy Policy applies to all products and services offered by us or the credit unions that use our services.

We keep this Privacy Policy under regular review and may update it from time to time to reflect changes in our practices, legal requirements or regulatory guidance.

Where we make changes:

- the updated version will be published on our website;
- where appropriate, we will provide a more prominent notice (for example, via email or service notifications) where changes are significant;

We will not make changes that materially reduce your rights under data protection law.

If you do not agree with any updates to this Privacy Policy, you may choose to stop using our services. Please note that this may affect our ability to provide certain products or services to you.

We encourage you to review this Privacy Policy periodically to stay informed about how we use your personal data.